일반논문-08-13-2-10

무선랜 메쉬 네트워크에서의 효율적인 멀티미디어 서비스를 위한 보안 정량화 기반의 프레임워크 연구

신 명 섭[a)‡], 임 선 희[a)], 이 옥 연[b)], 임 종 인[a)]

Study on Security Framework using Security Quantitative Analysis for the Effective Multimedia Services to WLAN Mesh Network

Myoung-Sub Shin[a)‡], Sun-Hee Lim[a)], Okyeon Yi[b)], Jongin Lim[a)]

요 약

최근 급격하게 사용이 증가되고 있는 멀티미디어 서비스는 QoS를 만족하기 위하여 네트워크의 속도, 잡음 환경, 단말의 계산 능력, 컨텐츠 종류 등을 기반으로 멀티미디어 데이터를 변환, 전송한다. 멀티미디어 서비스에서 정보 보호를 위해 중간 수준의 단일한 보안 서비스만을 제공하거나, 단말의 계산 능력 및 컨텐츠 종류에 따라 서비스 제공자 정책에 기반한 보안 메커니즘을 제공한다. 안전한 멀티미디어 서비스를 지원하기 위해 응용 계층의 보안과 네트워크 보안 메커니즘을 연구하여 보다 효과적인 멀티미디어 서비스를 위한 보안 메커니즘을 지원할 수 있다. 본 논문은 확장성과 경제성을 향상시킨 무선랜 메쉬 네트워크에서의 보안 수준, 침해 수준에 대한 효용 함수와 누적 보정 모델을 기반으로 멀티미디어 서비스 제공자가 단말의 계산 능력 및 컨텐츠의 종류 이외의 무선랜 메쉬 네트워크에서의 정량화된 보안 수준을 고려하여 멀티미디어 서비스의 보안 메커니즘을 결정하는 프레임워크를 정의한다.

Abstract

Multimedia service whose use is rapidly increasing supports effective services to convert and transmit multimedia data based on network speed, noise circumstance, terminal computation, and type of contents for satisfying QoS. For supporting information protection of multimedia service, it offers middle level of singular security service or security mechanism which is based on policy of service provider, depending on present terminal computation and type of contents. It can support security mechanism for more effective multimedia service, if we study security of application layer and network layer for supporting multimedia service

In this paper, we propose Multimedia security framework reflected on quantitative analysis of the WLAN(Wireless Local Area Network) mesh network security using the utility function in the level of the security, violation and addictive compensation model.

Keyword : WLAN Mesh Networks, Multimedia, Security Quantitative Analysis, Security

a) 고려대학교 정보경영공학전문대학원
Graduate School of Information Management and Security, Korea University
b) 국민대학교 자연과학대학 수학과
Department of Mathematics, Kookmin University
‡ 교신저자 : 신명섭(praise@korea.ac.kr)
"본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (IITA-2008-(C1090-0801-0025))

Ⅰ. 서 론

최근 급격하게 증가되고 있는 대용량 멀티미디어 서비스에서 정보 보호는 필수 요소이다. 그러나 대부분 획일적인 보안 메커니즘, 컨텐츠 종류에 따른 서비스 제공자의 정책

에 기반한 선택적인 보안 메커니즘이 제공된다. 무선 네트워크 서비스가 활발히 이용되고 있으며, 특히 무선랜 메쉬 네트워크는 중앙의 관리자에 의해 통제되지 않고 메쉬 라우터의 다양한 보안 메커니즘 제공으로 통신 경로에 따른 보안 수준이 다양하게 적용되고 있다. 이런 환경에서 멀티미디어 서비스의 획일적인 보안 정책은 QoS(Quality of Service)를 저해하거나 멀티미디어 데이터의 취약성을 야기할 수 있다.

ITU-T에서는 OSI(Open System Interconnection)에서의 안전한 서비스 제공을 위한 표준 참조 모델로서 OSI Security Architecture[1][2]를 정의한다. OSI Security Architecture에서는 인증(Authentication), 접근제어(Access Control), 무결성(Integrity), 기밀성(Confidential), 부인 방지(Non Repudiation)의 보안 서비스를 각 계층에서 제공한다[1]. 해당 보안 서비스는 각 계층의 특징과 보안 취약점을 바탕으로 한 계층에서만 구현되거나 여러 계층에서 제공된다. 각 계층에서 제공되는 보안 메커니즘을 통하여 제공되는 보안 서비스는 상호 보완적으로 다른 계층에도 영향을 주어 보안 서비스를 강화한다.

멀티미디어 데이터가 전송되는 과정에서 물리 계층, 데이터 링크 계층, 네트워크 계층에서의 보안 메커니즘을 통하여 인증, 기밀성, 무결성, 접근 제어 등의 보안 서비스가 제공된다. 동시에 멀티미디어 서비스가 정당한 사용자에 대한 안전한 서비스 제공을 위하여 멀티미디어 데이터 이용을 위한 인증, 기밀성, 무결성 등의 보안 조건을 요구하고 있다. 이를 기반으로 서비스 제공자가 네트워크 보안 메커니즘을 신뢰할 수 있을 경우, 멀티미디어 서비스 제공자는 계층별 보안 메커니즘의 결합을 통한 보안 서비스로 최적화된 멀티미디어 보안 서비스 제공이 가능하다. 따라서 무선랜 메쉬 네트워크에서 제공되는 보안 메커니즘의 특징을 정량 평가하고, 정량 평가 값을 기반으로 응용 계층에서의 멀티미디어 서비스의 보안 메커니즘을 결정하는 안전하고 효율적인 서비스가 가능한 멀티미디어 보안 프레임워크를 제안한다.

본 논문에서는 네트워크 경로 상에서 다양한 보안 수준이 가능한 무선랜 메쉬 네트워크에서의 보안 수준과 침해 수준을 정량화한 효용 함수와 누적 보정 모델을 기반으로 멀티미디어 서비스 요청시 전달된 네트워크 보안 메커니즘에 대한 정량화한 결과로 멀티미디어 서비스 제공자는 네트워크 환경에 기반을 둔 최적의 멀티미디어 보안 메커니즘을 도출할 수 있다. 본 논문은 제 2 장에서 차세대 광대역 서비스 제공을 위한 무선랜 메쉬 네트워크의 정의와 보안 메커니즘을 정의하고, 제 3 장에서 무선랜 메쉬 네트워크의 보안 요소를 정량적으로 평가한다. 제 4 장에서 무선랜 메쉬 네트워크 보안의 정량적 평가 값을 기반으로 한 안전하고 효율적인 멀티미디어 서비스 제공을 위한 멀티미디어 보안 프레임워크를 제안하고, 제 5 장에서는 제안한 멀티미디어 보안 프레임워크를 평가한다.

II. 무선랜 메쉬 네트워크 보안

무선랜 메쉬 네트워크는 무선랜을 기반으로 라우팅 기능을 포함한 기기를 통하여 다중 홉(multi Hop)을 통하여 WLAN 네트워크의 접근성이 향상된 네트워크 토폴로지이다. 무선랜 메쉬 네트워크는 최소한의 이동성을 가지고 기간망을 형성하는 Mesh Router와 단말인 Mesh Client로 구성되어 있다[3]. 무선랜 메쉬 네트워크는 IEEE 802.11 WGs[4]를 통하여 현재 표준화가 진행 중이다.

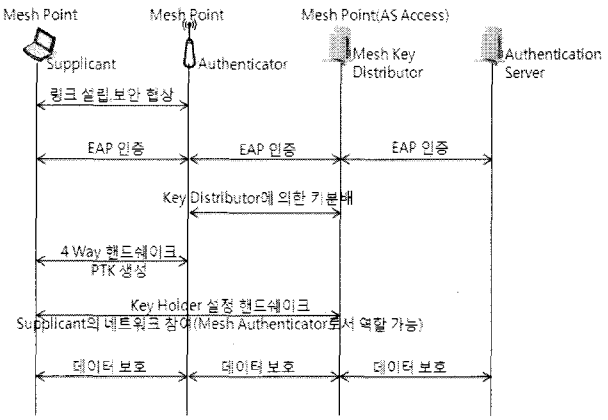


그림 1. 무선랜 메쉬 네트워크 보안 메커니즘
Fig 1. Security Mechanism of the WLAN Mesh Networks

무선랜 메쉬 네트워크는 메쉬 포인트(MP; Mesh Point)

의 인증 과정을 통하여 무선랜 메쉬 네트워크에 포함된다. IEEE 802.11i[5]에서 규정하고 있는 EAP[6] 기반 인증과 데이터 보호를 위한 CCMP 프로토콜을 확장 적용한다. 인증된 메쉬 포인트는 신뢰할 수 있는 노드로 무선랜 메쉬 네트워크에 참여한 다른 메쉬 포인트와 함께 경로 설정 및 데이터 전송을 수행한다. 각 메쉬 포인트는 인증자(Authenticator), 공급자(Supplicant) 역할을 같이 포함하고 있다. 또한 인증 및 키 분배의 효율성을 위하여 Mesh Key Distributor (MKD)를 통한 IEEE 802.11r 기반의 새로운 키 구조를 정의한다.

무선랜 메쉬 네트워크의 보안 메커니즘은 그림 1과 같은 과정으로 이루어진다. 인증 서버에 접근할 수 있는 MKD는 인증 서버에 인증이 된 후, 메쉬 포인트는 공급자의 역할을 하고 MKD가 인증자의 역할을 하여 인증 서버를 통하여 인증이 된다. 이 과정이 이루어진 후 공급자 역할을 하는 메쉬 포인트는 인증자로서의 기능을 할 수 있는 권한을 가진다.

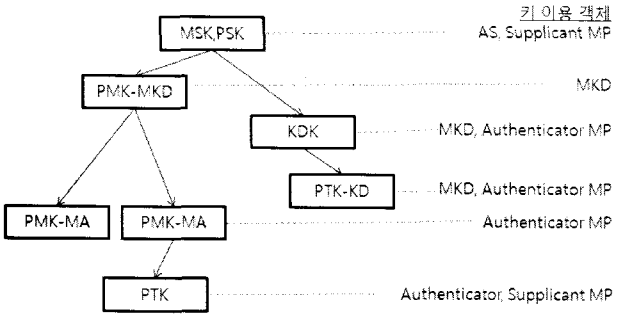


그림 2. 무선랜 메쉬 네트워크의 키 구조
Fig 2. Key Architecture of the WLAN Mesh Networks

통신을 하려는 두 노드는 공급자, 인증자로서 역할을 설정하고 보안 정책 협상을 통하여 결정을 하며 링크를 성립한다. 인증자 역할의 메쉬 포인트는 공급자 역할의 메쉬 포인트를 인증 서버를 통하여 EAP 프로토콜[6]을 기반으로 인증 과정을 수행한다. 공급자와 인증 서버 사이의 인증으로 생성된 키가 MKD로 부터 인증자 역할의 메쉬 포인트에 전달된다. 전달 받은 키를 이용하여 802.11i[5]에 정의된 4-way Handshake를 통하여 인증자 역할을 하는 메쉬 포인트와 공급자 역할을 하는 메쉬 포인트의 암호화 통신을 위한 비밀키 PTK를 생성한다. 메쉬 포인트가 Mesh Key Distributor와 보안 결합을 설립한 후, 메쉬 포인트는 키를 받고, 다른 메쉬 포인트에 대해 인증자로서의 역할을 한다.

새로운 키 구조는 그림 2와 같이 무선랜 메쉬 네트워크에 참여하는 새로운 메쉬 포인트 인증을 지원하기 위해 MKD로 부터 키를 분배 받기 위한 새로운 키를 정의하고 있다. 인증자 역할의 메쉬 포인트와 MKD에 의하여 PTK-KD를 발생하기 위한 키 Key Distribution Key(KDK)를 사용한다. PTK-KD는 MKD와 인증자로서의 메쉬 포인트 간의 안전한 통신을 위하여 사용된다. MKD는 인증자 역할의 메쉬 포인트에 PMK-MA를 전송하고 전달된 키는 다른 MA와 통신을 하기 위하여 인증자 역할의 메쉬 포인트에 의하여 이용된다.

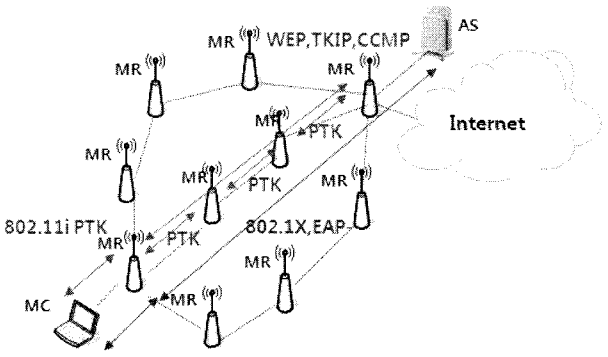


그림 3. 무선랜 메쉬 네트워크 보안
Fig 3. Security of the WLAN Mesh Networks

무선랜 메쉬 네트워크에서는 IEEE 802.1x[7]에서 정의하고 있는 인증자가 공급자를 각각의 포트로 관리하여 인증 서버로부터 각 포트별로 접속 허가 여부를 전달 받아서 접속 요구 단말의 네트워크 접근을 제어하는 포트 기반의 접근 제어(PACP)를 정의하고 있다. 단말은 메쉬 포인트가 공유하고 있는 802.11i[5]의 키를 사용하여 MAC(Medium Access Control) 계층에서 트래픽을 WEP, TKIP, CCMP를 통하여 무선 데이터의 기밀성, 무결성, 재공격(Reply Attack)방지를 제공한다.

Ⅲ. 무선랜 메쉬 네트워크 보안 수준의 정량적인 평가

무선랜 메쉬 네트워크는 단말과 무선 기지국이 직접 연결되어 있지 않고, 라우팅 기능을 가지고 있는 메쉬 라우터에 의하여 멀티 홉(multi hop)으로 연결되어 있다. 홉 마다 다양한 보안 메커니즘과 공격/보안 취약점은 네트워크 보안 평가를 위한 중요한 요소이다. 보안 메커니즘의 보안 강도, 공격/보안 취약의 침해 강도를 정의하고 이 값을 바탕으로 누적 보정 모델(Addictive Compensation Model)로 정량화된 보안 수준 값을 평가한다.

1. 무선랜 메쉬 네트워크 보안 메커니즘의 효용 함수(Utility function)

보안 메커니즘을 통하여 인증, 기밀성, 무결성, 접근제어, 부인 방지 등의 보안 서비스를 제공한다. 보안 메커니즘의 효용 함수는 보안 메커니즘에 의하여 수행되는 보안 서비스의 강도를 상대적으로 정량화하기 위하여 이용한다. 암호학적 알고리즘, 키의 길이, 인증서를 이용 및 양방향 인증 지원과 같은 요소들로 상대적 보안 강도를 정량화한다[8]. 정의된 보안 강도 값은 상대적인 값으로서 0 부터 4 까지의 정수 값을 적용한다. 무선랜 메쉬 네트워크에서의 MAC 계층 보안 메커니즘은 다양한 보안 서비스를 제공하고 있다. 다양한 보안 서비스에 대한 정량적 평가를 위해 행렬 구조의 효용 함수가 정의된다.

무선랜 메쉬 네트워크는 인증을 하지 않는 경우, 사전에 공유된 키를 이용한 인증, 인증 서버와의 연계를 통한 인증으로 나눌 수 있다. 인증 서버를 통한 인증은 802.1x[7], RADIUS 서버를 통한 사용자 인증이 가능하다[9]. EAP (Extensible Access Protocol)[6] 기반한 다양한 인증 방법이 가능해짐으로써 확장성 있는 인증 서비스를 제공한다. 사전에 공유된 키를 이용한 인증은 고정된 키 값을 사용함으로써 다양한 공격에 취약하므로 인증 보안 수준 값은 1이다. EAP-MD5는 해쉬 값을 이용하여 인증 서버로 사용자 인증을 수행하여 인증 보안 수준 값이 2, EAP-TLS는 클라이언트와 서버의 인증서를 사용하고 양방향 인증을 하므로 인증 보안 수준의 값은 4이다. EAP-TTLS, PEAP은 서버 인증시 인증서를 사용하고 클라이언트 인증시 인증서 또는 EAP, non-EAP를 이용하므로 EAP-TLS에 비하여 낮은 인증 보안 수준의 값인 3을 갖는다. 802.1x를 기반한 EAP-MD5, TLS, TTLS, PEAP는 WLAN 무선 메쉬 네트에서 인증 서버를 통하여 인증이 이루어지는 EAP 과정으로 802.1x 접근 제어가 이루어지므로 접근 제어의 보안 수준 값을 1로 정의한다.

표 1. WEP, TKIP, CCMP 비교
Table 1. Comparison of the WEP, TKIP, CCMP

	WEP	TKIP	CCMP
암호화 알고리즘	RC4	RC4	AES
무결성 알고리즘	CRC-32	Michael Algorithm	CBC-MAC
키 길이	40/104bit	128bit	128bit
패킷당 키	Key+IV	TKIP Key Mixing function	임시키(TK)

무선랜 메쉬 네트워크의 암호화 과정은 WEP, TKIP, CCMP이 있다[9]. RC4 암호 알고리즘 적용과 64 bit, 128 bit 키 생성의 취약점을 가진 WEP은 기밀성의 보안 수준 값은 1이다. 이에 반해 TKIP은 비교적 안전한 키 생성함수를 적용함으로써 WEP보다 높은 2를 갖는다. AES-CTR 모드를 적용한 CCMP는 가장 높은 기밀성 보안 수준 값인 4이다. WEP의 CRC(Cyclic Redundancy Check)-32는 무결성을 지원하기 위한 알고리즘이 아니다. 이 문제점을 개선한 TKIP은 Michael 알고리즘을 이용하여 64bit의 무결성 값 MIC을 만들어 암호화하여 전송을 하므로 WEP의 무결성의 보안 수준 값은 가장 낮은 1로 하고 TKIP은 2로 한다. CCMP는 CBC-MAC을 이용하여 가장 높은 무결성 보안 수준 값인 4로 한다.

무선랜 메쉬 네트워크에서 라우팅 과정에서 사용되는 프로토콜은 인증과 암호화 과정 후 라우팅이 이루어지므로 보안 서비스가 지원되지 않는 기본 값인 Hybrid Wireless Mesh Protocol (HWMP)를 기본으로 제공하고 있다. 그러나 라우팅 과정에서 라우팅 정보의 변조와 같은 문제가 이루어지므로 기존에 MANET에서 쓰였던 안전한 라우팅 기법의 도입이 요구된다. 추후 이용될 가능성이 높은 ARAN (Authenticated Routing for Ad hoc Networks)[10], SEAD

(Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Network)[11]에 대해 보안 서비스를 정량화한다. ARAN은 인증서를 기반으로 상호 인증이 제공되므로 인증의 보안 서비스 값을 3, SEAD는 행렬 기반의 Hash chain을 이용함으로써 이 값을 받은 노드들에 한하여 라우팅에 개입이 가능하므로 인증서에 비하여 행렬 값의 위조 가능성이 크므로 인증의 보안 서비스 값을 2로 한다. ARAN은 암호화하여 라우팅 정보를 경로의 객체가 보내므로 기밀성이 확보되므로 기밀성의 보안 서비스 값을 2로 한다. SEAD는 행렬의 Hash Chain 값을 통하여 무결성 값이 추가되므로 무결성의 보안 서비스 값을 2로 한다.

표 2. 무선랜 메쉬 네트워크 보안 효용 함수
Table 2. Utility Function of the WLAN Mesh Network Security

	보안 메커니즘	인증 Q_A	기밀성 Q_C	무결성 Q_I	접근제어 Q_{AC}
인증	Non	0	0	0	0
	Pre-Shared Key Authentication	1	0	0	0
	802.1x, EAP-MD5	2	0	0	1
	802.1x, EAP-TLS	4	0	0	1
	802.1x, EAP-TTLS	3	0	0	1
	802.1x, PEAP	3	0	0	1
암호화	Non	0	0	0	0
	WEP	0	1	1	0
	TKIP	0	2	2	0
	CCMP	0	4	4	0
라우팅	Non	0	0	0	0
	ARAN	3	2	0	0
	SEAD	2	0	2	0

2. 무선랜 메쉬 네트워크 공격/보안 침해 사항의 효용함수(Utility function)

무선랜 메쉬 네트워크의 구성 요소인 메쉬 라우터의 경우는 물리적 보안에 대한 취약성 및 제한된 자원으로 보안 강화가 어렵다. 동시에 DoS 공격의 경우는 근본적인 해결책이 미비하여 추후에 유사한 공격에 노출될 가능성이 크다. 따라서 이런 공격 유형이 어떤 보안 서비스를 침해하는지를 공격/보안 침해 사항을 정량화하여 보안 수준 정량화 시 반영하는 것이 필요하다. 무선랜 메쉬 네트워크의 공격 및 보안 침해 사항을 상대적으로 정량화하기 위해 보안 침해 사항에 대한 강도를 효용 함수로 정의한다. 무선랜 메쉬 네트워크의 공격 및 보안 침해의 보안 서비스는 크게 인증, 기밀성, 무결성, 가용성으로 나눈다. 공격/보안 침해 사항은 대표적인 경우로 방해 전파 공격, DoS 공격, 데이터 도청, 라우팅 정보 변경, 네트워크 구조 변경이 있다. 방해 전파 공격과 DoS 공격은 네트워크 이용을 침해하므로 가용성의 보안 서비스 값을 1로 정의한다. 데이터 도청은 정보가 공개되어 기밀성이 침해되므로 기밀성의 보안 서비스 값을 1로 정의한다. 라우팅 정보 변경은 데이터의 무결성이 침해되므로 무결성의 보안 서비스 값을 1로 정의한다. 네트워크 구조 변경은 구조의 변경으로 인하여 노드의 단절과 관련하여 가용성의 보안 서비스 값을 1, 의도적으로 다른 노드에 정보가 통과하도록 하여 정보 노출이 가능하므로 기밀성의 보안 서비스 값을 1로 정의한다.

표 3. 무선랜 메쉬 네트워크 공격/보안 침해 효용 함수
Table 3. Utility function of the WLAN Mesh Network Attack/Security Violation

	인증 V_A	기밀성 V_C	무결성 V_I	가용성 V_{AV}
방해 전파 공격	0	0	0	1
DoS 공격	0	0	0	1
데이터 도청	0	1	0	0
라우팅 정보 변경	0	0	1	0
네트워크 구조 변경	0	1	0	1

3. 누적 보정 모델(Addictive Compensation Model)

누적 보정 모델(Addictive Compensation Model)은 보안 메커니즘과 공격/보안 침해 사항을 하나의 값으로 정량화하기 위한 모델로서 보안 메커니즘을 정량화하는 누적 보상 모델(Additive Award Model)과 공격/보안 침해 사항을 정량화하는 누적 벌점 모델(Additive Penalty Model)로 구성된다. 누적 보상 모델은 개별적인 보안 메커니즘, 보안 서비스의 혼합을 통하여 보안 특징의 향상을 누적해서 정량화한다[8].

무선랜 메쉬 네트워크 보안 P는 일련의 인증, 암호화, 라우팅 기능을 제공하는 과정으로서 보안 서비스인 인증, 기밀성, 무결성, 접근 제어 4가지 보안 서비스를 제공한다. 이용하는 서비스에 따라 보안 서비스 중요도의 상이함, 인증, 암호화, 라우팅 각 과정에서 독립적으로 정의한 효용 함수 값, 각 과정이 단계적으로 이루어짐으로써 전후 관계에 의하여 중요도의 고려가 필요하다. 보안 서비스 중요도, 각 과정의 독립적인 효용함수 값, 전후 관계를 중요도를 고려하여 보안 메커니즘의 보안 특징을 누적하여 정량화한 누적 보상 모델 $\sigma(P)$은 다음과 같다.

- A(.): 인증 기능을 제공하는 과정에서의 각 보안 요소의 보안 수준
- E(.): 암호화 기능을 제공하는 과정에서의 각 보안 요소의 보안 수준
- R(.): 라우팅 기능을 제공하는 과정에서의 각 보안 요소의 보안 수준

아래의 변수는 각 과정에서 인증 Q_A , 기밀성 Q_C, 무결성 Q_I, 접근 제어 Q_{AC} 에 대한 보안 서비스를 지칭한다. 예를 들어, A_{Q_C} 는 인증 과정에서 보안 서비스로서 기밀성의 보안 수준을 지칭한다.

$$\begin{bmatrix} A_{Q_A} & A_{Q_C} & A_{Q_I} & A_{Q_{AC}} \\ E_{Q_A} & E_{Q_C} & E_{Q_I} & E_{Q_{AC}} \\ R_{Q_A} & R_{Q_C} & R_{Q_I} & R_{Q_{AC}} \end{bmatrix} \begin{bmatrix} W_{Q_A} \\ W_{Q_C} \\ W_{Q_I} \\ W_{Q_{AC}} \end{bmatrix} = \begin{bmatrix} P_A \\ P_E \\ P_R \end{bmatrix}$$

멀티미디어 서비스 제공자 입장에서 보안 서비스 요소 중에서 인증, 기밀성, 무결성, 접근제어 중에서 접근 제어의 경우는 네트워크 제공자 입장에서 중요한 요소로서 보안 서비스의 정량적인 평가에서 중요한 요소로 고려하지 않을 수도 있고, UCC(User Created Contents)와 같은 공개된 컨텐츠와 같이 기밀성과 관련된 사항이 중요한 요소로 고려되지 않을 수도 있으므로 가중치 값을 이용하여 이러한 사항을 반영하도록 한다. W(.)는 각 보안 요소별 중요도에 대한 가중치 상수이다. 각 요소에 대해 특정 사항이 다른 요소에 절대적으로 영향을 받지 않도록 보정하기 위하여 상수는 $W_{Q_A} + W_{Q_C} + W_{Q_I} + W_{Q_{AC}} = 1$의 조건을 만족해야 한다. 위의 행렬식을 기반으로 인증, 암호화, 라우팅 과정에 대한 인증, 기밀성, 무결성, 접근 제어에 대한 보안 수준과 가중치의 곱을 기반으로 각 과정에 대한 보안 서비스를 누적하여 정량화한 값 P_A, P_E, P_R를 도출한다.

$$[P_A P_E P_R] \begin{bmatrix} w_A \\ w_E \\ w_R \end{bmatrix} = \sigma(P)$$

인증, 암호화, 라우팅 과정은 순차적으로 발생하는 과정으로서 선후 관계의 중요성과 각 과정에 대해 독립적으로 정의한 효용 함수 값의 반영을 위하여 가중치 상수 w(.)를 사용한다. 단 각 요소에 대해 특정 사항이 다른 요소에 절대적으로 영향을 받지 않도록 보정하기 위하여 상수는 $w_A + w_E + w_R = 1$의 조건을 만족해야 한다. 인증, 암호화, 라우팅 각 과정에 대한 보안 서비스를 누적한 값에 가중치 w(.)를 곱함으로써 보안 메커니즘 P를 한 개의 값 $\sigma(P)$로 정량화한다.

기존의 공격 및 보안 침해 요소가 복합적으로 작용하여 취약 사항을 강화시킨다. 누적 벌점 모델은 개별적인 공격 및 보안 침해 사항의 혼합을 통하여 보안 침해 사항을 누적해서 정량화 한다. 무선랜 메쉬 네트워크 공격/보안 침해 사항 V는 인증, 기밀성, 무결성, 가용성 4가지 보안 서비스를 침해한다. 이용하는 서비스에 따라 보안 서비스 중요도의 상이함의 고려가 필요하다. 보안 서비스 중요도를 고려하여 공격/보안 침해 사항의 침해 사항을 누적하여 정량화한 누적 벌점 모델 $\tau(V)$은 다음과 같다. 공격 및 침해 요소 V는 m개의 공격 및 침해의 결합을 통하여 이루어진다.

- V_A^J : j 번째 수행에서 인증 서비스와 관련된 공격 및 침해 수준
- V_C^J : j 번째 수행에서 기밀성 서비스와 관련된 공격 및 침해 수준
- V_I^J : j 번째 수행에서 무결성 서비스와 관련된 공격 및 침해 수준

- V_{AV}^{J} : j 번째 수행에서 가용성과 관련된 공격 및 침해 수준

v(.)는 각 공격 및 침해 수준별 중요도에 대한 가중치 상수이다. 아래의 변수는 인증 A, 기밀성 C, 무결성 I, 가용성 AV에 대한 보안 서비스를 지칭한다. 각 요소에 대해 특정 사항이 다른 요소에 절대적으로 영향을 받지 않도록 보정하기 위하여 상수는 $v_A+v_C+v_I+v_{AV}=1$의 조건을 만족해야 한다. 공격/보안 침해 사항에 대한 보안 서비스 효용 함수 값에 가중치 v(.)를 곱하여 누적하여 공격 및 침해 요소 V를 한 개의 값 $\gamma(P)$로 정량화한다.

$$\tau(V)=\sum_{j=1}^{m} v_A V_A^j + v_C V_C^j + v_I V_I^j + v_{AV} V_{AV}^j$$

다양한 요소를 반영한 가중치($W_{Q_1}, W_{Q_2}, W_{Q_3}, W_{Q_{1C}}, w_A, w_E, w_R, v_A, v_C, v_I, v_{AV}$)를 기반으로 한 누적 보상 모델과 누적 벌점 모델을 통하여 보안 메커니즘과 공격/보안 침해 사항을 평가한다. 누적 보정 모델(Addictive Compensation Model)은 누적 보상 모델과 누적 벌점 모델을 하나의 값으로 통합한다. 누적 보정 모델을 이용하는 주체에 따라서 보안 메커니즘, 공격/보안 침해 사항의 중요도 반영을 위하여 β, ρ라는 가중치를 이용한다. 보안 메커니즘 P와 공격/보안 침해 V의 누적 보상 모델과 누적 벌점 모델과 가중치 β, ρ를 곱하여 한 개의 값 $ACM(P,V)$로 정량화한다.

$$ACM(P,V)=\beta \cdot \sigma(P)-\rho \cdot \gamma(V)$$

무선랜 메쉬 네트워크는 멀티 홉으로서 각 홉의 누적 보정 모델 $ACM(P,V)$의 값 중 최소값으로 라우팅 경로상의 보안 메커니즘과 공격/보안 침해 사항을 정량화한다.

Ⅳ. 무선랜 메쉬 네트워크 보안 환경 인식 기반의 멀티미디어 보안 프레임워크

무선랜 메쉬 네트워크에서 정당한 권한을 가진 사용자에 대한 서비스 제공을 위한 인증, 기밀성과 무결성 제공의 데이터 보호, 안전한 데이터 전송을 위한 경로 설정의 라우팅이 이루어진 이후에 멀티미디어 서비스가 제공된다. 기존의 멀티미디어 서비스 제공자는 단일한 보안 메커니즘을 제공하거나, 단말의 계산 능력과 컨텐츠의 종류에 따른 네트워크 서비스와 독립적인 멀티미디어 보안 메커니즘을 제공하고 있다. 이런 응용 서비스와 네트워크 서비스의 보안 설계의 독립성은 중복된 보안 서비스의 자원으로 인한 overhead가 발생하거나 보안 서비스의 미비로 안전성의 문제를 가질 수 있다. 이를 개선하기 위해 단말의 계산 능력과 컨텐츠 종류 이외에 무선랜 메쉬 네트워크 보안 메커니즘과 기존 공격/보안 침해 사항을 누적 보정 모델(ACM)을 통하여 반영함으로써 최적의 멀티미디어 보안 메커니즘을 결정할 수 있는 멀티미디어 보안 프레임워크를 제안한다.

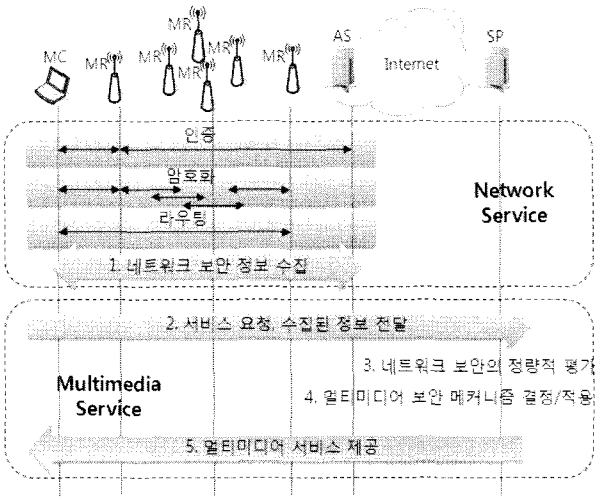


그림 4. 네트워크 환경에서 멀티미디어 보안 제공 과정
Fig 4. Multimedia Security Process in the Network

본 멀티미디어 보안 프레임워크는 보안 메커니즘과 기존 공격/보안 침해 사항을 라우팅 과정에서 수집, 수집된 정보를 통하여 앞 장에서 정의한 보안 수준의 정량적인 평가값을 도출, 도출된 값을 반영한 멀티미디어 서비스의 암호화 알고리즘, 키 길이, 암호화 적용 대상을 네트워크 보안 환경 적응적으로 결정하는 부분으로 구성된다.

1. 보안 메커니즘과 공격/보안 침해 정보 수집

멀티미디어 서비스 제공자가 멀티미디어 데이터의 보안 메커니즘을 결정하기 위하여 무선랜 메쉬 네트워크 보안 메커니즘과 기존 공격/보안 침해 사항의 수집이 필요하다. 무선랜 메쉬 네트워크는 단말과 무선 기지국이 직접 연결되어 있지 않으므로 라우팅 과정에서 각 노드에 대한 정보를 수집한다. 보안 메커니즘은 보안 협상 과정의 정보 또는 크로스 레이어(Cross Layer) 기반으로 정보를 수집하고, 공격/보안 침해 사항은 침입 탐지 시스템의 정보를 기반으로 정보를 수집한다. 메쉬 클라이언트와 라우터는 그림 5와 같이 인증, 암호화, 라우팅 과정에서의 보안 메커니즘과 공격/보안 침해 정보를 다음과 같은 객체를 통해 이용할 수 있다.

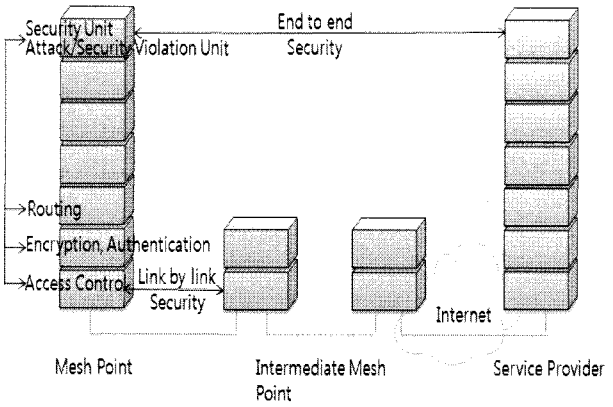


그림 5. 메쉬 클라이언트, 라우터의 객체 구조
Fig 5. Node Structure of the MC, MR

메쉬 클라이언트는 인접한 노드에 Security Unit, Attack/Security Violation Unit에 의하여 보관된 정보를 라우팅시 RREQ(Route Request) 메시지를 통하여 라우팅 정보와 함께 각 메쉬 라우터들은 경로의 인증, 암호화에 대한 보안 메커니즘 정보와 공격/보안 침해 정보를 인터넷에 직접 연결된 메쉬 라우터에 전송을 한다. 수집된 보안 메커니즘의 정보와 공격/보안 침해 정보는 RRES(Route Response) 메시지를 통하여 메쉬 클라이언트에게 전달되어 필요한 정보를 수집하게 된다.

2. 응용 계층에서 멀티미디어 보안 메커니즘 결정

멀티미디어 서비스 제공자는 보안 메커니즘과 공격/보안 침해 정보를 서비스 요청 과정에서 전달 받고, 그림 6과 같이 전달받은 정보를 바탕으로 서비스 제공자의 정책 기반으로 컨텐츠의 종류에 따라 각 가중치 값을 제공 받아 보안 메커니즘과 공격/보안 침해 사항을 효용 함수와 누적 보정 모델을 통하여 하나의 정량적인 값 누적 보정 모델(ACM)을 계산한다. 멀티미디어 제공자는 ACM 값, 단말의 계산 능력과 컨텐츠 종류를 기반으로 멀티미디어 서비스에 제공될 보안 메커니즘을 결정한다.

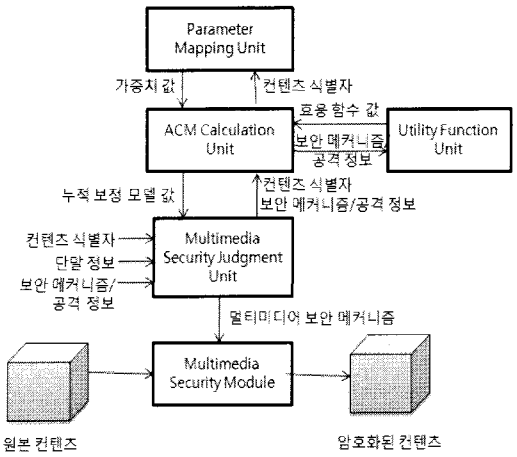


그림 6. 멀티미디어 보안 프레임워크
Fig 6. Multimedia Security Framework

멀티미디어 서비스 제공자는 다음과 같은 객체를 이용하여 멀티미디어 보안 프레임워크를 구성한다.

- Utility Function Unit: 전달 받은 보안 메커니즘과 공격/보안 침해 요소 정보를 효용 함수를 이용해서 변환하는 객체
- Parameter Mapping Unit: 요청한 멀티미디어 컨텐츠에 기반을 두어 ACM 계산에 필요한 가중치를 결정하는 객체
- ACM Calculation Unit: 가중치와 효용함수 값을 가지고 네트워크 보안 수준의 정량화한 값인 ACM을 계산

하는 객체

- Multimedia Security Judgment Unit: ACM 값과 단말의 계산 능력, 요청 멀티미디어 컨텐츠에 기반하여 보안 메커니즘을 결정하는 객체
- Multimedia Security Module: 결정된 보안 메커니즘에 의하여 멀티미디어 서비스에 보안 메커니즘을 적용하는 객체

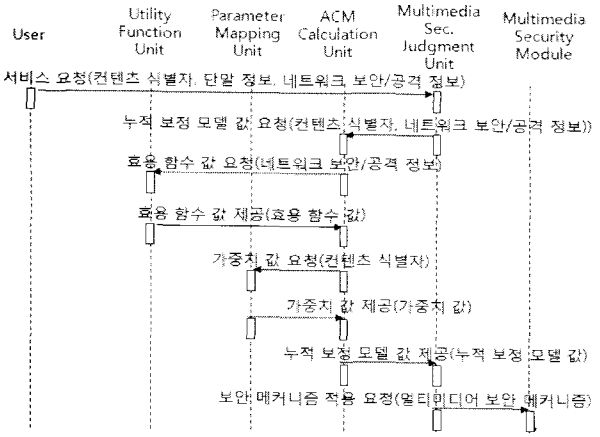


그림 7. 멀티미디어 보안 프레임워크 흐름도
Fig 7. Flow of the Multimedia Security Framework

멀티미디어 보안 프레임워크의 운영되는 절차는 그림 7과 같다. 사용자로부터 컨텐츠 식별자, 단말 정보와 보안 메커니즘, 공격/침해 정보를 전달 받아서 ACM Calculation Unit에 정보를 전달해준다. ACM Calculation Unit는 보안 메커니즘과 공격/침해 정보에 대응되는 효용 함수 값을 Utility Function Unit에서 전달받고 컨텐츠에 대응되는 ACM 값의 적용에 필요한 가중치 값을 Parameter Mapping Unit을 통해서 전달 받는다. 전달 받은 효용 함수 값과 가중치 값을 기반으로 ACM 값을 구하여 Multimedia Security Judgment Unit에 전달한다. Multimedia Security Judgment Unit은 전달 받은 ACM 값과 컨텐츠 정보에 기반하여 자신의 정책기반으로 멀티미디어 보안 메커니즘을 결정하여 Multimedia Security Module에 전달한다. Multimedia Security Module은 전달받은 메커니즘을 기반으로 보안 메커니즘을 적용하여 서비스를 제공한다.

본 논문에서는 다양한 멀티미디어 서비스 중 시간에 따라 연속적으로 변화하는 동영상을 포함한 멀티미디어 압축(compression), 전송(transmission) 및 표현(description) 에 관한 국제 표준인 MPEG(Motion Picture Experts Group)에 대한 보안 서비스 기반으로 연구한다. MPEG 비디오 데이터는 비디오를 구성하는 최소 단위인 프레임 단위로 구성되어 있고, 이를 적당한 크기의 GOP(Group of Picture)로 묶어서 처리한다. 또한 I 프레임(Intra frame; GOP의 독립성을 확보하게 하는 프레임내의 부호화 프레임), P 프레임(Predicted frame;프레임간의 순방향 예측 부호화 프레임), B 프레임(Bidirectional Frame;프레임간의 쌍방향 예측 부호화 프레임)의 세 가지의 프레임을 정의하여 과거의 재생 영상으로부터 순방향 예측과 미래의 재생 영상으로부터 역방향 예측을 사용하는 양방향 예측을 한다[12].

멀티미디어 보안 서비스로서 암호화와 관련된 사항으로서 암호학적인 알고리즘과 키 길이, 암호화 적용 대상 등이 있다[13][14][15]. 멀티미디어 서비스의 기밀성과 관련하여 기존 암호학적 알고리즘과 키 길이를 기반으로 무차별 대입 공격(brute force attack)에 강인함을 기준으로 한 보안 강도는 표 4와 같다[9].

표 4. MPEG 암호 보안 강도[16]
Table 4. Security Strength of the MPEG Encryption Algorithm[16]

정책	알고리즘	키 길이	보안 강도
A1	DES	56	1
A2	AES-128	128	2
A3	RC6	128	3
A4	3-DES	168	4
A5	AES-192	192	5
A6	AES-256	256	6

MPEG 비디오 암호화 적용 대상으로 MPEG 인코딩 속성을 기반으로 4 가지 수준을 제공하고 있다[13]. I, P, B 모든 헤더를 암호화 하는 방법, 모든 헤더와 I 프레임을 암호화 하는 방법, 모든 I 프레임과 P 프레임과 B 프레임의 I 블록을 암호화 하는 방법, 모든 프레임을 암호화 하는 방법이다. 4 가지 수준은 영상 복호화시 중요한 요소를 기준으로 프레임의 헤더 값, I 프레임, I 블록 등의 요소의 추가를 통하여 암호화 적용 대상을 확장함으로써 보안 수준을 다르게 하고 있다. 각 방법은 암호화 하는 멀티미디어 데이터양이 큰 차

이를 보내고 있고, 표 5와 같이 I, P, B의 모든 헤더를 암호화 하는 것이 보안 강도가 가장 낮고, 모든 프레임을 암호화 하는 것이 보안 강도상 가장 강하다고 할 수 있다.

표 5. MPEG 암호화 적용 대상의 보안 강도
Table 5. Security Strength of the MPEG Encryption Method

정책	암호화 적용 대상	보안 강도
S1	I, P, B의 모든 헤더의 암호화	1
S2	모든 헤더와 I 프레임 암호화	2
S3	모든 I 프레임과 P, B프레임의 I 블록 암호화	3
S4	모든 프레임 암호화	4

Multimedia Security Judgment Unit은 단말의 계산 능력에 기반으로 암호학적 알고리즘과 키 길이, 암호화 적용 대상의 가능 범위를 결정하고, 일반적인 무선랜 메쉬 네트워크 환경의 보안 메커니즘에 대한 기준 누적 보정 모델 값 ACM_{basis}에 대응되는 컨텐츠 종류 C에 따른 멀티미디어 보안 수준 값 PN_{basis}을 확인한다. 멀티미디어 서비스를 이용하는 현재 무선랜 메쉬 네트워크의 보안 메커니즘에 대해 ACM Calculation Unit에 의해 계산된 누적 보정 모델 값 $ACM_{evaluation}$에 대응되는 보안 수준 값 $PN_{evaluation}$를 도출한다. 기준 네트워크 환경에 비해 높은 보안 수준일 경우 낮은 멀티미디어 보안 수준을 제공하고, 낮은 보안 수준일 경우 높은 멀티미디어 보안 수준이 제공되어야하므로 각 값이 선형적으로 반비례하므로 다음과 같은 식을 도출한다.

$$\frac{1}{ACM_{basis}} : \frac{1}{ACM_{evaluation}} = PN_{basis} : PN_{evaluation}$$

멀티미디어 서비스 제공자는 컨텐츠 종류에 따른 요구사항을 반영한 가중치 값 τ, υ를 암호학적 알고리즘과 키 길이의 정책 Ai(i=1, 2, ... 6), 암호화 적용 대상의 정책 Sj(j=1, 2, 3, 4)의 보안 강도와의 조합을 통해 도출된 값 $PN(A_i, S_j) = \tau \cdot PN(A_i) + \upsilon \cdot PN(S_j)$과 $PN_{evaluation}$의 값의 차가 최소인 멀티미디어 보안 메커니즘을 선택한다. $\min|PN(A_i, S_j) - PN_{evaluation}|$ 이 선택된 멀티미디어 보안 메커니즘에 기반을 두어 멀티미디어 서비스 제공자의 정책 기반하여 누적 보정 모델의 값이 높을 경우 보안 강도가 낮은 암호학적 알고리즘과 키 길이, 암호화 적용 대상을 선택하고, 누적 보정 모델의 값이 높을 경우 보안 강도가 낮은 암호학적 알고리즘과 키 길이, 암호화 적용 대상을 선택할 수 있다.

V. 제안한 멀티미디어 보안 프레임워크의 평가

기존에 단일한 멀티미디어 보안 메커니즘 또는 단말의 계산 능력, 컨텐츠의 종류에 기초하여 정책 위주의 일부 한정된 멀티미디어 보안 메커니즘을 제공한다. 기존 멀티미디어 보안 프레임워크의 경우는 유선의 네트워크와 같은 일정한 보안 수준을 제공하는 환경에서는 큰 문제가 되지 않는다. 그러나 무선랜 메쉬 네트워크의 경우는 라우팅을 통하여 다양한 보안 메커니즘을 제공하는 경로를 통하여 통신이 이루어지고, 경로에 따라 다양한 보안 수준을 제공한다. 선택된 QoS를 제공하는 경로의 보안 수준에 대한 보장이 없는 상황에서 일반적인 네트워크 보안 환경을 고려한 멀티미디어 보안 메커니즘은 낮은 보안 수준을 제공하는 경로에서는 멀티미디어 데이터가 네트워크 상에서 공격에 취약하여 노출되고, 강한 보안 수준을 제공하는 경로에서는 네트워크상의 강한 보안 서비스로 멀티미디어 데이터가 안전함에도 멀티미디어 데이터의 강한 보안 수준을 제공하는 보안 메커니즘으로 인하여 QoS를 저해한다.

제안한 멀티미디어 보안 프레임워크는 무선랜 메쉬 네트워크 보안 메커니즘과 공격/보안 침해 사항 정보를 기반을 효용 함수를 이용하여 보안 서비스별 보안 수준과 침해 수준을 정량적으로 평가하고, 컨텐츠 종류에 따른 보안 서비스, 과정, 보안/침해 사항의 중요성을 고려한 가중치와 효용 함수 값을 이용한 누적 보정 모델을 통해 무선랜 메쉬 네트워크의 보안 수준의 정량적 평가 값을 도출해서 멀티미디어 보안 메커니즘을 결정하는 과정에서 단말의 계산 능력과 컨텐츠의 종류와 더불어 반영한다. 또한 기존의 연구에서 보안 수준 평가가 네트워크적인 관점에서 다양한 요소를 선형 누적만 했으나. 본 논문에서 무선랜 네트워크 보안 수준 평가 과정에서 다양한 종류의 멀티미디어 서비스의 요구 사항에 따른 객체의 인증, 기밀성, 무결성 등의 보안 서비스의 요소 중요성에 기반한 가중치 값을 반영한 네트

워크 평가를 통해 각 컨텐츠에 적합한 네트워크 평가가 가능하다. 이를 통해서 멀티미디어 데이터가 전송되는 유동적인 네트워크 보안 환경에 따른 적응적인 멀티미디어 보안 메커니즘을 제공한다.

실제 중간 수준의 보안 서비스를 제공하는 무선랜 메쉬 네트워크의 보안 수준 평가 값인 기준 누적 보정 모델 값에 대응되는 멀티미디어 데이터의 보안 수준에 기반을 두어, 서비스가 제공될 무선랜 메쉬 네트워크 환경의 보안 수준 평가 값에 대응되는 멀티미디어 보안 수준을 도출한다. 도출된 멀티미디어 보안 수준에 해당하는 멀티미디어 데이터의 암호화 알고리즘, 키 길이, 적용 대상을 결정하여 무선랜 메쉬 네트워크의 보안 환경에 따른 최적화된 멀티미디어 보안 메커니즘의 제공이 가능하다. 즉, 멀티미디어 보안 프레임워크는 낮은 보안 수준을 제공하는 경로에서 멀티미디어 데이터의 높은 보안 수준의 멀티미디어 보안 메커니즘을 통해 안전한 서비스를 제공하고, 강한 보안 수준을 제공하는 경로에서는 낮은 수준의 멀티미디어 보안 메커니즘을 통해 QoS를 향상시킨다.

Ⅵ. 결 론

멀티미디어 서비스는 대부분 획일적인 보안 메커니즘 또는 컨텐츠 종류에 기반을 둔 일부 선택적인 보안 메커니즘을 제공한다. 네트워크의 보안 환경이 일정 수준일 경우 기존의 멀티미디어의 보안 정책은 문제가 되지 않는다. 무선랜 메쉬 네트워크는 빠른 데이터 전송 속도를 통하여 다양하고 고품질의 서비스를 제공하는 것이 가능하다. 그런데 무선랜 메쉬 네트워크는 메쉬 라우터의 다양한 보안 서비스 제공 능력으로 인하여 무선랜 메쉬 네트워크 통신 경로에 대한 보안 수준은 다양하다. 그럼으로써 멀티미디어 서비스의 획일적인 보안 정책은 때로는 강한 보안 정책으로 인하여 QoS를 저해하거나 낮은 보안 정책으로 인하여 멀티미디어 서비스의 안전한 서비스 제공을 할 수 없는 결과를 가져올 수 있다. 따라서 무선랜 메쉬 네트워크 보안 환경 인식을 기반으로 한 멀티미디어 서비스 제공이 필요하다.

본 논문에서는 무선랜 메쉬 네트워크의 인증, 암호화, 라우팅 과정에서의 보안 서비스와 이전의 공격/보안 취약 정보를 라우팅 과정에 수집한다. 수집된 정보를 멀티미디어 서비스 요청시 제공받고, 전달받은 정보를 추가 보정 모델을 통하여 보안 서비스와 취약점을 정량화한다. 이 과정에서 멀티미디어 서비스 제공자는 정책 기반으로 인증, 기밀성, 무결성, 접근 제어의 보안 요소와 보안 서비스와 취약점의 중요도 기반의 가중치를 제공한다. 이렇게 무선랜 메쉬 네트워크의 보안의 정량화된 값을 기반으로 멀티미디어 서비스의 암호화 알고리즘과 키 길이, 적용 대상을 조절하여 안전하고 효율적인 멀티미디어 서비스를 제공한다.

현재는 멀티미디어 보안 메커니즘은 암호 알고리즘, 키 길이와 프레임, 헤더 등의 적용 대상 조절을 통하여 제공을 하였으나 향후 연구에서는 지그재그(Zigzag) 코딩과 같은 다양한 인코딩 환경의 형식 양립적인 암호화(Format-compliant Encryption) 및 지각적인 암호화(Perceptual Encryption)다양한 멀티미디어 암호화 기반을 둔 네트워크 보안 환경 고려를 통해 최적화된 멀티미디어 보안 프레임워크가 연구되어야 할 것이다.

참 고 문 헌

[1] International Telecommunication Union (ITU), Security Architecture for Open Systems Interconnection for CCIT Applications, Recommendation ITU-T X.800, ITU, Geneva, 1991.

[2] International Organization for Standardization (ISO), Information Processing Systems－Open Systems Interconnection－Part 2: Security Architecture, ISO/IEC 7498-2, ISO, Geneva, 1989.

[3] Akyildiz, I.F., Wang, X. and Wang, W., "Wireless Mesh Networks: A Survey," Computer Networks Journal (Elsevier), Vol. 47, pp. 445-487, March 2005.

[4] W.Steven Conner, Jan Kruys, Kyeongsoo Kim, Juan Carlos Zuniga, "IEEE 802.11s Tutorial; Overview of the Amendment for Wireless Local Area Mesh Networking." IEEE 802 Plenary, November 2006

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

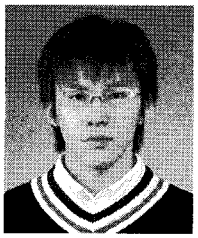
[6] RFC 3748, "Extensible Authentication Protocol(EAP)," June 2004

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

[8] Avesh K. Agarwal, Wenye Wang, "On the Impact of Quality of Protection in Wireless Local Area Networks with IP Mobility,"

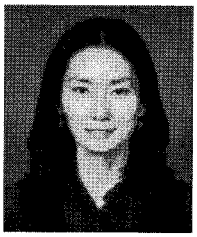
Springer Mobile Network Application, Vol. 12, pp. 93-110, November 2006
[9] Stedano M. Faccion, Carl W Ijting, Jarkko Kneckt, Ameya Damle, "Mesh WLAN Networks: Concept and System Design," IEEE Wireless communication, Vol. 13, pp. 10-17, April, 2006
[10] Kimaya Sanzgiri, Daniel Laflamme, Bridget Dahill, "Authenticated Routing for Ad hoc Networks," In journal on Selected Areas in Communication, Vol. 23. pp. 598-610, March 2005
[11] Yih-Chun Hu, David B. Johnson, Adrian Perrig, "Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," In proceedings of the 4th IEEE workshop on Mobile Computing Systems and Application, Vol. 1, pp.175-192, July 2003
[12] Atul Puri, Xuemin Chen. Ajay Luthra, "Video coding using the H.264/MPEG-4 AVC compression standard," Signal Processing: Image Communication Vol. 19, No. 99, pp. 793-839, October 2004
[13] L.Tang, "Methods for Encrypting and Decrypting MPEG Video Data Efficiently," Proceeding of ACM International Multimedia Conference and Exhibition, pp. 219-229, Noberber 1996
[14] Guang Ming Hong. Chun Yuan, Yi Wang, Yu Shuo Zhong, "A Quality Controllable Encryption for H.264/AVC Video Coding," Advances in Multimedia Information Processing PCM 2006, Vol. 2461, pp. 510-517, October 2006
[15] Tuo Shi, Brian King, and Paul Salama, "Selective Encryption for H.264/AVC Video Coding," the Society of Photo-Optical Instrumentation Engineers, Vol. 6072, pp. 461-469, Feb, 2006
[16] Chui Sian Ong, Klara Nahrstedt and Wanghong Yuan, "Quality of Protection for mobile multimedia Application," in ICME 2003, Vol.2, pp. 137-140, July 2003
[17] Martin Prangl, Tibor Szkaliczki, Hermann Hellwagner, "A Framework for Utility-Based Multimedia Adaptation," IEEE Trans. on circuits and systems for video technology, Vol. 17, pp. 719-728, June 2007

저 자 소 개



신 명 섭

- 2006년 2월 : 고려대학교 공과대학 전자공학과 졸업
- 2006년 9월 ~ 현재 : 고려대학교 정보경영공학전문대학원 석사과정
- 주관심분야 : 무선 이동 통신, 정보 보호, 보안 정량화



임 선 희

- 1999년 2월 : 고려대학교 컴퓨터학과 졸업
- 2005년 2월 : 고려대학교 정보보호대학원 석사
- 2005년 3월 ~ 현재 : 고려대학교 정보경영공학전문대학원 박사과정
- 주관심분야 : 무선 통신, 정보 보호

이 옥 연

- 1988년 2월 : 고려대학교 수학과 졸업
- 1990년 2월 : 고려대학교 이학석사
- 1996년 8월 : Univ. of Kentucky Ph.D
- 1999년 ~ 2001년 : ETRI 선임연구원
- 2001년 ~ 현재 : 국민대학교 수학과 조교수
- 주관심분야 : 이동통신 정보보호, 컴퓨터 보안

저 자 소 개

임 종 인

- 1980년 2월 : 고려대학교 수학과 졸업
- 1982년 2월 : 고려대학교 수학과 석사
- 1986년 8월 : 고려대학교 수학과 박사
- 1986년 ~ 1999년 :고려대학교 수학과 교수
- 1999년~현재 : 고려대학교 정보보호대학원 원장, CIST 센터장
- 주관심분야 : 정보 보호 정책, 암호 이론