모바일 게임 파트너 선정을 위한 보안프로토콜 검증

신 승 중 (중부대학교 컴퓨터공학부 정보보호관리학전공 교수)

요약

사용자 기반이 활성화 되고있는 모바일에서 게임을 지속적으로 유지하기 위해 전자서명과 공개키 분배 및 인증 등의 기능이 포함된 메시지전송 프로토콜로 구현된 프로그램의 검증문제를 Choquet 퍼지적분을 이용하여 해결하고 이를 퍼지적분과 비교분석하였다. 기능별로 보안기술, 보안정책, 전자문서처리, 전자문서전송, 암 · 복호화키로 나누어 분류하여 구현된 내용을 기능별점수와 전문가의 요구사항을 구현된 프로토콜에서 산출 값과 비교하여 메시지 보안프로토콜을 기능별로 점수화하여 검증하였다.

Abstract

The objective of this paper was to cope with the verification of the message transfer protocol that integrates the electronic signature and the distribution and authentication of public key in Mobile Game using m-Commerce Choquet fuzzy integral compared with fuzzy integral. They were classified into the security technology, the security policy, the electronic document processing, the electronic document transportation and the encryption and decryption keys in its function. The measures of items of the message security protocol were produced for the verification of the implemented document in every function.

1. 서론

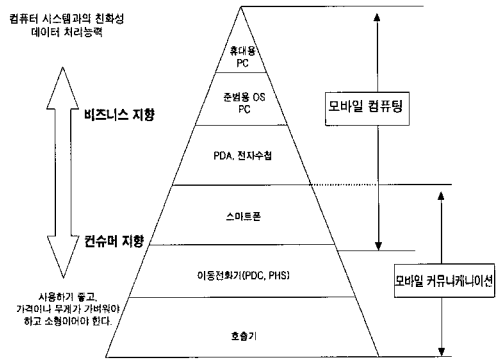
모바일폰의 급성장으로 기업간의 경쟁이 치열해 지면서 조직의 생산성 증대와 효율화를 위한 정보시스템의 역할이 더욱 중요해지고 있다. 특히 글로벌시대의 생각과 속도의 변화가 중요한 문제로 부각되면서 핵심기술인 암 · 복호화 문제를 구사하는 분야부터 대형 시스템의 물리적인 관리까지 총체적인 개념에서 문서의 전달은 매우 중요한 문제라 할 수 있다. 그러므로 사용상의 문제점으로 위 · 변조, 처리속도, 송수신확인, 메시지보안 등을 말한다. 또한, 전자서명이나 암호방식에 의한 당사자간의 인증절차의 알고리즘 확인이며 이러한 방법으로 네트웍 상에 자신과 상대를 서로 확인하는 과정을 말하며 이러한 것을 '증명한다'라고 말할 수 있다.[2]

IMT-2000에서 빈번히 일어날 수 있는 전자 서명과 공개키 분배 등 인증상의 문제를 도출해 내어 이를

해결하기 위한 방안으로 메시지를 안전하게 보내는 방법과 기존 연구를 통해 이에 대한 처리과정을 비교하여 정책에 대한 성능 및 기능 검증을 통한 보다 효율적인 방법이 필요하다. 현재 미국에서 개발한 MSP(Message Security Protocol)에 대한 기술을 기본으로 하여 전자문서처리 및 전자서명에 관한 기본 사항과 이에 따른 제반 사항을 작성하고, 우리 실정에 입각하여 실용적이고 법적인 문제와 전자문서를 암호화하고 전자서명과 수신자 확인서의 발급으로 완벽한 전자문서 관리 시스템을 구현하는데 본 연구의 목적이 있다.[10] [11]

현재 모바일에서의 문서이동이 급증하고 있고 앞으로 IMT-2000에서는 지속적으로 무선기반에 대한 연구가 여러 분야에서 활발히 이루어지고 있는 실정이다. 이는 문서를 Web상에서 안전하게 전달하는 것이 최고의 과제라 하겠다.

이러한 추세에 부합하기 위한 일환으로 모바일 환경에서 게임을 즐길 수 있으며, 기존의 안전성을 고려한 네트워크게임프로토콜의 개발을 위한 방법으로 기존의 MSP 프로토콜보다 무선 환경에서 효율적인 결과를 도출시키고자 GNP(Game Network Protocol)를 설계하였다. 그리고 GNP는 본 연구자가 개발하였던 CMP(Cryptography Message Protocol)를 무선환경에 맞도록 새로운 아이디어를 첨삭하였다. 또한 제안된 프로토콜의 성능을 검증하기 위하여 보안 프로토콜의 대표적인 기능들을 선별하여 그 기능들을 퍼지적분을 이용하여 검증하였다. 기능별로 MSP와 GNP를 비교하여, 각 기능별의 차이점을 도출 및 비교를 통한 차이점을 구체적으로 살펴보면서 보안기술에서 소항목에 해당하는 기밀성과 무결성, 송신부인봉쇄, 수신부인봉쇄를 설문지에서 추출한 값으로 그 차이를 분석하여 각 기능을 비교하였다. 정책에 의한 구체적인 내용에서도 메시지 보안등급 제한, 메시지 접근 보안등급, 다중등급보안에 대하여 MSP에서의 차이점과 GNP에서 처리되는 사항을 비교하였다.



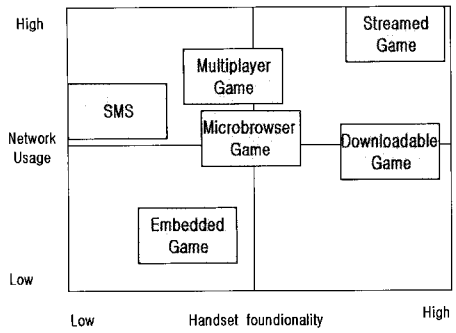
[그림 1] 모바일 컴퓨팅 터미널의 종류와 현황

2. MSP와 GNP의 구조

2.1 최근 동향

무선인터넷 환경의 개선으로 다양한 서비스 제공이 가능해지고, 게임 컨텐츠 개발업체들이 아케이트(오락실게임) 및 온라인 게임에서 모바일 게임(Mobile Game)으로 영역을 확대하고 있어, 네트워크 사업자나 단말기 제조업체들이 모바일 게임 산업을 주목하고 있다. 즉, 네트워크 사업자는 모바일 게임 개발업체와 비즈니스 모델 개발을 위해 관계를 강화시키고 있으며, 단말기 제조업체는 네트워크 사업자, 포털(Portal), 게임 개발업체 등 과의관계 강화를 위한 전략을 구축하고 있다.

유형	내용
Embedded	단말기가 제조될 때부터 게임이 내장됨, 게임을 할 때 네트워크 트래픽이 발생하지 않는 특징을 가지고 있으며, 네트워크를 통해 게임을 업데이트 할 수 있음
SMS	문자 메시지를 통해 상호간에 게임을 즐길 수 있음(예:퀴즈게임)
Microbrowser	WAP기반으로 간단한 그래픽과 애니메이션을 제공하지만, 네트워크 사용에 한계가 있음.
Multiplayer	네트워크에 접속하여 여러 사람이 'Virtual Games World ' 상에서 서로 대전하며 즐길 수 있음.
Downloadable	단말기에 자바 기반으로 게임을 다운로드 받은 후 단말기 단독으로 혹은 네트워크에 접속하여 게임을 즐길 수 있음
Streamed	네트워크를 통해 실시간으로 스트림 액션을 즐길 수 있는 게임으로, 현재의 이동통신 네트워크에서는 즐기기 어려우나 무선랜(Wireless LAN)으로는 단말기 상에서 즐길 수 있음.



[그림 2] 모바일 게임의 유형과 포맷

2.2 MSP의 구조

MSP는 메시지의 인증과 무결성, 기밀성, 부인봉쇄, 배달증명 등을 포함한 보안기술을 포함시켜 NSA의 주도하에서 개발 되었다. 이러한 MSP의 기본 구조는 암호화된 메시지를 헤딩 (Security Heading)하는 것으로 특히, 상호연결 개방시스템은 이기종 시스템이나 서로 다른 운영체제 하에서도 안전하게 메시지를 전달하는 기능을 구현하기 위한 구조이다. [그림 3]의 MSP의 구조 내용을 국제 표준 기구의 표준안과 비교하면 [표 1]과 같다[2][3][4].

구조	MSP		
	메시지전송		검색
기능	헤딩(Heading)	MSP내용	각 메시지별 캡슐화
	정보처리시스템	상호연결 개방시스템	안전한 자료네트워크시스템
	메시지전송	키관리	인 증
	메시지핸드링	보안프로토콜	디렉토리, 메일 프로토콜

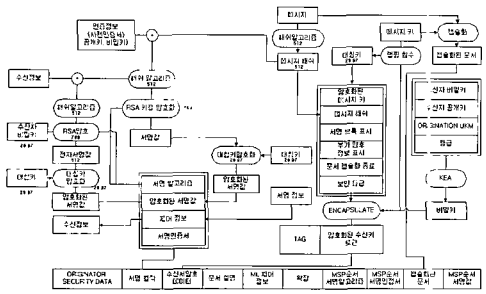
[그림 3] MSP의 구조와 기능

메시지 전송시스템은 통신 프로토콜 위에 정보의 누출을 방지하는 프로토콜을 이용하여 구현되는 시스템으로 [표 1]의 여러 기능이 구현되도록 설계되어 보안성 및 안전성이 보장되어야 하기 때문에 미 국방성에서는 보안 제품의 기준을 정리 하고 있다. 또한, [표 1]의 보안제품 기준안에는 MSP가 포함 되어 있

형태	내용	기준안 구분
정보처리시스템	개방시스템상호연결- 보안구조	ISO 7498/2
상호연결 개방시스템	CCITT 응용을 위한 기본참고모델, 변환문 요약의 상세화, 변화문 요약을 위한 기본암호규칙의 상세화	CCITT X.200 CCITT X.208 CCITT X.209
메시지운용	서비스와 시스템의 요약, 메시지전송시스템 요약정보서비스의 정의 및 절차, 프로토콜의 상세화, 메시지 시스템	CCITT X.400 CCITT X.411 CCITT X.419 CCITT X.420
훈령집	Models. 인증의 기본틀	CCITT X.501 CCITT X.509
메일전송프로토콜	J. B. Postel, August 1982	RFC821
ARPA 사용메시지의 기본틀을 위한 표준안	D. Crocker, 13 August 1982	RFC822
안전한자료 망구성시스템	메시지보안프로토콜, SDNS MSP 이용을 위한 훈령의 상세화, X.400 Rekey Agent Protocol. 접근기능개념의 문서, 접근기능의 상세화, 키관리프로토콜의 상세화	SDN.701 SDN.702 SDN.703 SDN.801 SDN.802 SDN.903
미 국방부의 보안제품 기준안	서비스 기본 배경과 지원부분 프로토콜의 내용 및 정의와 분류사항 메시지전송을 위한 요구조건 전송시스템의 접근요구 사항 전송시스템의 접근요구 사항	MIL-STD-2045-18500

[표 1] MSP 관련 기준안 비교표

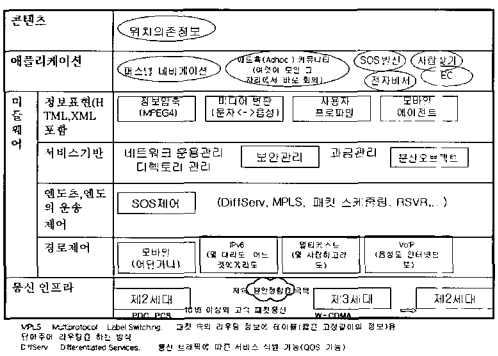
으며, MSP에 사용되는 DES나 RSA는 미국 상무성 표 준국(NBS : 현재의 NIST)이 1977년에 제정 발표한 표준암호 방식[4]으로, 1993년에 제정된 인터넷의 PEM(Privacy Enhanced Mail)의 표준으로 사용되고 있다. 이러한 MSP 프로토콜은 기존의 X.400 MTS에 투명성을 제공 하고 MSP 보호 서비스를 위한 MSP UA와 기능 개체 (Functional entity)들로 구성되어 있으며 [그림 5]와 같은 기본 골격으로 구성되어 있다. MSP는 대형 시스템에서 주로 운영되며 등급 보안을 다중화 하기 위하여 비밀등급카드를 이용하여 접근자를 통제하고 있고 수신자의 인증표(Certificate), 사용자주요자료(UKM), 보조벡터(Auxiliary vector, AV)를 얻기 위해 X.501과 X.509의 디렉토리 시스템을 이용하는 특징을 가지고 있다.



[그림 4] MSP 프로토콜

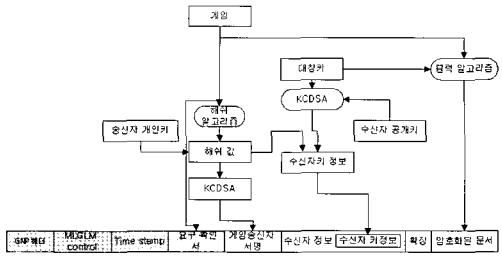
2.3 GNP의 구조

본 연구에서 설계된 GNP는 일괄처리로 인한 시간 소모를 해결하고 이기종 간에 메시지 전달을 원활히 하며 접근카드 미사용/클라이언트의 PC사용 가능성/메시지의 전달 여부를 서버에서 알 수 있도록 하였다. 구체적으로 메시지를 헤더프로토콜에 탑재하여 메시지를 전송하는 단계를 중점적으로 연구하였으며 미국방부 보안제품 기준안과 CCITT의 표준안에 따른 메시지 전송 요구사항, 송수신 프로토콜의 상세화, 인증의 개념을 추가하였다. GNP 1, 2, 3은 일괄처리로 인한 시간소모를 제거하기 위해 문서를 중요도 등급별로 구분하여 처리하도록 설계되어 전자문서 교환의 효율성을 증대시킬 수 있으나 다양한 접근자들에 대한 복잡한 관리가 요구된다. 이러한 다중 관리를 위한 부수적 시스템 관리를 최소화하기 위해 문서 등급을 미리 분류하여 처리하는 합리적 기능을 설계에 반영하였다.



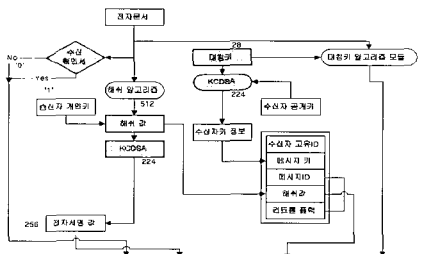
[그림 5] GNP의 기본개념도

또한 게임메시지 접근의 통제 수단으로 사용되는 카드를 제거하기 위해 MLGLP(Multi Layer Game Link Protocol, 이하 MLGLP)기능을 이용함으로써 클라이언트 시스템을 PC급 시스템으로 대체할 수 있게 되었다. MLGLP는 GNP 헤더에 Switching System을 부착하여 메시지가 기능별, 문서 내용별, 주요 사양별로 처리될 수 있도록 세 가지 형태로 개발되었다.



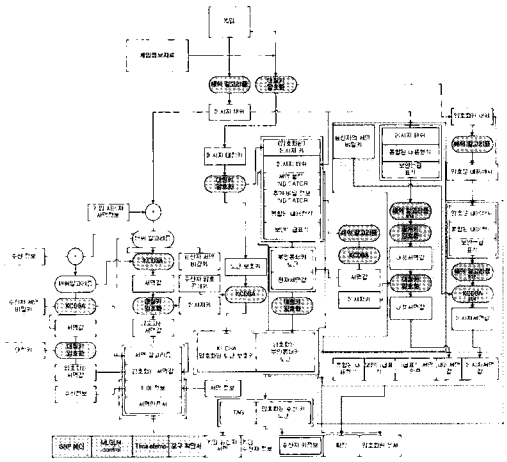
[그림 6] GNP3 프로토콜

[그림 6]의 GNP3는 문서의 복잡도와 시스템 트래픽에 따라 문서를 구분하고 보안 등급에 따라 처리하도록 하였다. 이러한 전자문서관리시스템을 암호화 방법이 간단하고 보다 신속한 업무처리 지원할 수 있는 장점이 있어 단순한 메시지, 서신, 공지사항 등에 사용 할 수 있다. GNP3는 전자문서를 1회 암호화하고 이를 수신자 키 정보에 수록하여 전송함으로써 간단하지만 안전성을 고려한 프로토콜이다.



[그림 7] GNP2 프로토콜

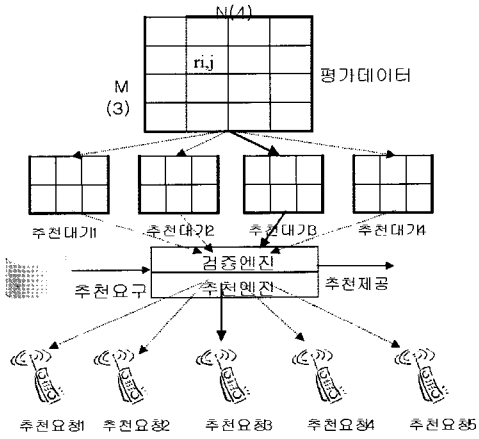
[그림 7]의 GNP2는 MSP의 메시지 헤더 부분에 전체 정보가 아니라 송수신자 암호 데이터의 해쉬값만을 전송하도록 단순화시킨 전자문서관리시스템이다.



[그림 8] GNP1 프로토콜

GNP2는 암호화 및 복호화가 용이하고 대체로 안전하게 문서 처리를 할 수 있는 프로토콜로 비교적 단순하면서 보안성을 요구할 때 사용된다. GNP2는 대외비 또는 어느 정도의 비밀성을 유지해야하는 문서처리를 위해 설계된 프로토콜이다. [그림 8]의 GNP1은, MSP의 메시지 헤더 부분에 있는 송수신자 데이터를 암호화, 캡슐화하여 기록하는 확장부분을 일부 수정한 프로토콜이다. GNP1은 완벽한 1급 비밀 또는 국가기밀 정보를 취급, 전송할 때 사용할 수 있도록 설계된 프로토콜로 안전성 유지를 위한 복잡한 암호화 처리, 캡슐화를 위한 송수신자 정보의 탑재, 암호문서에 요구확인서 부분 추가 등을 고려하여 설계되었다.

이러한 GNP1은 해쉬 알고리즘을 이용한 전자서명의 검증과 GNP 헤더 생성을 위한 복잡한 과정으로 인해 처리 시간이 지연되는 단점이 있으나 취급되는 문서의 보안 처리 문제가 더 중요한 경우에는 유용하다. [그림 9]은 제안된 프로토콜의 처리 과정과 구조를



[그림 9] GNP 프로토콜

도시한 것으로 GNP1,2,3을 결합하여 재 설계한 것이다. 각각의 ①평가 데이터를 이용하여 검증엔진에서 비교하여 헤더를 따로 분리하여 메시지를 전송하기 위하여 ②추천엔진으로 보내진 자료 및 게임 참가자를 추천하여 매칭을 한다. ③게임 수준에 따라서 분류를 할 수 있는 프로토콜이다.

2.4 MSP와 GNP의 분석

MSP는 대형시스템 내에서 구현되었고 GNP는 중·소형 서버에서 운영될 수 있도록 설계하였다. 간단한 구조에서 복잡한 암호화를 거쳐 만들어진 문서를 전송하는 헤더이다. [표 2]는 GNP와 MSP의 헤더 기능을 비교한 것으로 헤더 보유, 수신자 암호데이타, 암호화된 전자문서, 문서 각 기능을 캡슐화하여 확장부분에 탑재하는 기능이 공통적이다.

헤더기능	GNP	MSP	비고
게임명 헤더보유	o	o	
서명블럭		o	
수신자암호데이타	o	o	
요구확인서	o		
메세지 보안등급 및 분류처리	o		
서명알고리즘		o	
메세지 목록		o	
암호화된 전자문서	o	o	
확장	o	o	
키정보	o		

[표 2] 항목별 헤더기능 비교표

MSP 헤더의 서명블럭, 서명알고리즘, 메시지 목록은 문서 내용과 문서 이용자의 정보를 비교하여 접근의 범위를 미리 조절하는 기능으로 이를 처리하기 위해 초대형 시스템과 접근자 관리시스템이 필요하다. 반면 GNP의 요구확인서, MLML, 키정보는 현재 보유하고 있는 시스템에서 다중 처리 기능을 지원하도록 설계되었다.

한편 MSP와 GNP의 기능을 종합적으로 비교한 결과는 [표 3]과 같다. 먼저 헤더 사용 시 여러 기능을 탑재하여 속도, 시스템 사용시간, 데이터로드 및 처리시간을 각각 비교한 결과 전송처리시간에 있어서는 GNP가 처리의 단순화로 다소 빠른 것으로 예상되었다. 한편 MSP는 접근자 처리에 있어 접근자 관리 시스템에서 키 관리에 따른 접근자의 개별정보를 요구하고 있으나 GNP는 비밀키를 업무 처리자에게 별도 부여함으로써 간단히 처리할 수 있다. 또한 MSP의 보안 전송 기능은 OSI 참조 모델의 응용계층에서 처리되도록 설계되었다.

구 분	MSP	GNP1	GNP2	GNP3	비 고
전송처리시간	MSP	++	+,-	-	
공개키암호화 알고리즘	RSA	KCDSA	KCDSA	KCDSA	군수품 수출 규제로 국내 표준 사용
비밀키암호화알고리즘	DES	SEED	SEED	-	규제
해쉬값	MD5	MD5	MD5	MD5	
메시지 헤더	전체정보	전체정보	송수신정보	키정보	class 이용
문서전송	전체전송	전체전송	일부정보전송	내용위주전송	
위변조확인	확인	recv_stemp;	recv_stemp;	recv_stemp;	
송·수신 확일		분류	-	-	통합관리가능
인증서비스	접근자의 정보에 따라 인증제공	송·수신자 정보로 인증 관리	송·수신자 정보로 인증 관리	송신자서명에 의해 인증	
키관리	접근시 카드사용	비밀키	비밀키	비밀키	
보안기능 전송기반	OSI에서의 응용층 이용	SSL이용	SSL이용	SSL이용	

[표 3] MSP와 GNP 비교표

또한 GNP는 SSL(Secure Socket Layer)을 이용함으로써 보다 안전한 전송이 이루어질 수 있도록 설계되었으며 메시지가 GNP에 등록되면 문서 등급에 따라 선택되어질 프로토콜로 로드되어 메시지 앞에 헤더값이 붙도록 하였다.

3. GNP의검증및고찰

본 논문에서 제안된 프로토콜과 게임네트워크프로토콜과의 비교우위를 검증하기 위하여 Choquet 퍼지적분을 이용하였다. 적용된 퍼지적분은 어떤 대상이 여러 항목에 대해서 평가되고 각 평가 항목의 중요도에 차이가 있을 때 이들에 대한 평가치를 종합하는데

번호	대항목	소항목	점수	분류	MSP(h(x)	GNP(h(x)		
					1	1	2	3
1	게임보호기술	기밀성	0.05380	B	0.99	0.99	0.91	0.88
2		무결성	0.04782	C	1.00	1.00	0.98	0.97
3		송신부인봉쇄	0.04136	C	0.90	0.91	0.90	0.88
4		수신부인봉쇄	0.04878	C	0.92	0.92	0.91	0.90
5	게임보호정책	메세지 등급 제한	0.04830	C	0.00	0.90	0.90	0.90
6		메세지 분류 처리	0.04734	C	0.00	0.99	0.98	0.98
7		메세지 접근 등급	0.05236	B	0.00	0.98	0.50	0.00
8		다중등급보안	0.04854	C	0.99	0.00	0.00	0.00
9	게임문서관리	수신자확인서	0.03778	D	0.98	0.98	0.91	0.00
10		전자서명	0.05786	B	0.95	0.94	0.94	0.00
11		수신자키정보	0.04423	C	0.88	0.90	0.89	0.00
12		암호화된 전자문서	0.04902	C	0.99	0.99	0.55	0.23
13	게임전송확인	송수신자확인	0.04902	C	1.00	1.00	1.00	0.00
14		내용 위·변조확인	0.05595	B	0.97	0.98	0.95	0.00
15		송·수신시간확인	0.04089	C	1.00	1.00	1.00	1.00
16		인증및 인증서확인	0.05691	B	0.00	0.00	0.00	0.00
17	게임보증키	RSA	0.07030	A	1.00	0.00	0.00	0.00
18		KCDSA	0.04160	C	0.00	1.00	1.00	1.00
19		DES	0.06647	A	1.00	0.00	0.00	0.00
20		SEED	0.04160	C	0.00	1.00	1.00	1.00

[표 4] 게임등급별 문서에 따른 데이터와 퍼지척도

유효하다. 따라서 보안 프로토콜에 대한 비교분석에서 고려해야할 게임보호기술, 게임보호정책등의 여러 항목에 대한 비교우위를 검증하는 데에 적용하였다. 먼저 분석할 게임네트워크 프로토콜이 갖추어야 할 조건을 결정한 다음 각 조건의 상대적인 중요도를 결정할 수 있다. 퍼지적분을 적용하기 위하여 보안을 위한 메시지 프로토콜의 기능적인 부분을 항목별로 분류하여 빈도분석을 한 내용을 [표 4]에 나타내었다. 특히 게임보호기술, 게임보호정책, 게임문서관리, 게임전송, 게임보증키의 다섯가지 항목으로 분류하고, 각 항목에 대해 세부항목을 작성하였다. 위에서 제시된 프로토콜의 기능별 통계표 의하여 다음에 나타나 있는 항목에 따른 퍼지척도의 결과를 [표 4]에 나타내었다. 분류에 의한 감을 병의 등급은 퍼지적분의 부분집합을 구성 및 정규화과정을 위해 편의상 A, B, C, D로 분류하였다.

구분 / 종류	MSP	GNP1	GNP2	GNP3
FUZZY INTEGRAL 에 의한 방법	0.667660	0.713550	0.612170	0.370200
CHOQUET FUZZY INTEGRAL 에 의한 방법	0.165381	0.218206	0.203884	0.135293

[표 9] MSP와 GNP의 결과비교

수게노(Sugeno)의 일반적인 퍼지적분의 정의는 다음과 같다.

$$\int_X h(x) \circ g(\cdot) = \sup_{E \subseteq X} \mathrm{Min}[\min_{x \in E} h(x), g(E)]$$

그리고 적용된 Choquet 퍼지적분은 다음과 같이 정의된다.

$$\int_X h(x) \circ g(\cdot) = \sum_{i=1}^{n} h(x_i)[g(A_i) - g(A_{i+1})]$$

여기서 h(x)는 데이터에 대한 MSP와 GNP의 처리결과이고 g(x)는 각 항목에 대한 척도이다. 먼저 퍼지적분에 의한 방법에서는 GNP1에 의한 방법이 가장 우수한 것으로 나타나 있다. 반면에 Choquet에 의한 방법에서는 GNP1과 GNP2에 의한 방법이 우수한 것으로 나타나 있다.

GNP3는 MSP에 비하여 알고리즘의 제한 규모가 작고 MSP는 항목에 의한 알고리즘이 골고루 배치되어 있으므로 상기와 같은 결과를 볼 수 있다.

4. 결론

본 논문에서는 미국의 MSP의 메시지 처리환경을 보완하고, 다양한 기반하에서 사용 할 수있도록 다중등급 보안을 토대로 이를 우리나라의 시스템환경에 적합하도록 네트워크 게임 프로토콜(GNP)을 인터넷 기반에서 응용하여 개발하였다. 이를 사용하여 각각의 게임에 차등을 적용하여 합리적인 방법으로 게임에서 생성되는 메시지를 처리하도록 하였다. 또한, MSP와 GNP의 프로토콜의 검증을 위하여 퍼지적분을 이용하여 수행하였다.

이로서 게임알고리즘으로 구성된 프로그램은 수시로 보완될 수 있도록 SCM의 절차를 준수하고 이를 통하여 관리하는 프로토콜은 외부에서 침입하고자하는 의도에 따라 제한된 사항을 준수하고 갈수록 지능화되어 가는 시스템보호 측면에서 지속적인 연구가 요구되며, 이를 검증하기 위해서 Choquet 퍼지적분을 사용하여 MSP와 GNP의 등급별, 항목별의 결과값에 다소 차이가 있는 것을 확인할 수 있다. 또한 각 문서에 따른 평가데이터의 구성에 있어서 보다 효율적인 면에서 구성이 보완되어야 할 것으로 보고, 아직까지는 GNP의 보안 평가치가 다소 낮은 것을 볼 수 있으나, 앞으로 이를 바탕으로 새로운 보안 서비스 설계 및 구현에 많은 참조가 되기를 바라며 향후 지속적

인 형상관리와 개발 및 분석을 통하여 좀 더 편리하고, 안전한 합리적인 보안 서비스 설계가 이루어져야 할 것으로 사료된다.

참고문헌

[1] Menezes, Handbook of Applied Cryptography, CRC Press, pp.1-6, 1997.

[2] 정보보호센타, 정보보호뉴스 22호, 한국정보보호센타, pp2, 1999.

[3] 정보보호 심포지움 '99, "인증관리 센터 구축 및 운영계획" 1999.

[4] H. Feistel, "Cryptography and Computer Privacy, "Scientific A merican, pp.15-23, 1973.

[5] National Bureau of Standards, Data Encryption Standard, U.S. FI PS PUB49, pp. 17-18, 1977.

[6] A. Simmizu and S.Miyaguchi, "Fast Data Encipherment Algorithm F EAL, "Eurocrypt'87, pp. 267-278, 1987.

[7] 한국 정보 보호 센터, "인증 업무 준칙, "한국 정보 보호 센터 내부 자료, 1999.

[8] 정보통신부,"정보보호산업발전대책(1998-2002)", pp70-77, 1997.

[9] 한국전자통신 연구원, "인터넷 상거래의 물결", 한국전자통신 연구원, pp128-129, 1998.

[10] http://www.kisa.or.kr/pds/att/missi.hwp

[11] http://www.imc.org/workshop/sdn701.txt 1994.

[12] Caption J. Detombe CD, A Comparison of Two Protocols - PEM vs MSP, 7th ACCSS, May, 1995.

[13] http://www.imc.org/workshop/sdn701.txt 1997.

[14] http://www.armadillo.huntsville.al.us/index.html

[15] 신승중, 박인규 "퍼지적분을 이용한 메시지 프로토콜 검증" vol.3, no7, 한국정보처리학회, 2000

[16] 신승중, 김현수 "보안문서 전용 메시지 프로토콜구현" vol. 2, no 2, 한국DB학회, 2000

[17] http://www.itfind.or.kr/ 주간IT동향 1043호, ISSN1225-6447, 2002.04.24