論 文

V.42 bis 모뎀의 새로운 구조

正會員 姜 昌 求* 正會員 曺 洪 根** 正會員 金 大 榮*

Enhanced Architecture of the V.42 bis Modem

Chang Goo Kang,* Hong Keun Cho,** Dae Young Kim* *Regular Members*

要 約

최근 공중통신망 혹은 전용 회선망에서 모뎀을 이용한 고속 데이타 통신이 증가하고 있으며 CCITT V.42 bis에 기초한 데이타 압축 기술이 CCITT V.42 오류 정정 기능을 가진 모뎀에 대하여 적용되고 있다. 이러한 모뎀 기술에 있어서 새로운 관심사로 등장하고 있는 또하나의 기능은 전송데이타의 비인가적 노출에 대한 정보보호 기능이다.

본 논문에서는 오류 정정 기능과 데이타 압축 기능을 가진 모뎀에 정보보호 기능을 추가한 모뎀의 새로운 구조를 제안하고 제안한 모뎀의 효율적 동작을 위하여 기능정의, 서비스 프리미티브 정의 및 동작절차를 상세히 기술하였다.

ABSTRACT

In recent high-speed data modems for use over PSTN or leased line, the data compression technique based on CCITT V.42bis Recommendation is of popular use along with CCITT V.42 error control function. A remaining concern to advanced-application users is the protection against unintended eavesdropping.

This paper proposes the architectural model on how the security mechanism should be adopted into the above mentioned error-correction /data compression modems.

Also, the functional definitions and the operational procedures are described in detail for possible implementation.

I. 개 요

데이타 통신의 증가와 함께 공중전화망 혹은 전용 회선망을 통한 데이타 단말기(DTE : Data Terminal Equipment) 간 데이타 통신에 있어서 모뎀을 이용한 비동기 데이타 전송이 증가하고 있다.

이러한 비동기 데이타 전송에 있어서 요구되는 중요한 세가지 특성은 첫째 전송선로상의 오류발생에 대한 오류 정정 특성, 둘째 데이타 전송효율을 높이

*忠南大學校 電子工學科
Dept. of Elec. Eng. Chung Nam Univ.
**韓國電力公社 技術研究員
論文番號 : 92-143(接受1992. 8. 8)

기 위한 데이타 압축 특성, 셋째 전송 데이타에 대한 비인가적 노출로부터 정보를 보호하는 정보 보호 특성을 들 수 있다.

첫번째 오류 정정 특성에 대해서는 일반적으로 DTE 간에 오류 정정을 위하여 Kermit, ASCII 등과 같은 비동기 통신 프로토콜을 DTE에서 사용하고 있으나 그림 1과 같은 구성에서는 모뎀이 오류 정정 특성을 가지고 있는 것이 더욱 바람직하다. 따라서 CCITT V.42에서는 모뎀에서 비동기 데이타를 동기 데이타로 변환하고 LAPM(Link Access Procedure for Modem) 프로토콜을 이용한 오류 정정 절차를 권고하고 있다.[1]

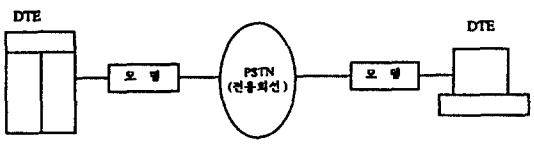


그림 1. 모뎀을 이용한 데이타 통신
Fig. 1. Data communication using modems

두번째 데이타 압축 특성에 대해서는 CCITT V.42 bis에서 오류 정정 기능을 갖는 DCE(Data Circuit Terminating Equipment)에 대한 데이타 압축 절차를 권고하고 있으며 이러한 데이타 압축절차를 이용하여 전송 효율(throughput)을 향상시킬 수 있다.[2]

세번째 정보보호 특성에 대해서는 오류 정정 기능과 정보보호 기능을 가진 혼합부호 및 데이타 압축기능과 정보보호 기능을 갖는 혼합 부호들이 개발 되었다.[3]-[6] 그러나 일반적으로 데이타 단말기와 모뎀사이에 별도의 암호장치를 삽입하여 전송데이타의 기밀성을 보호하고 있다. 이러한 암호장치가 오류 정정 특성이 없는 모뎀과 함께 사용될 때 전송로상에서 오류가 발생되면 오류전파현상이 생길수 있으므로 이에 대한 보호대책이 요구된다. 일반적으로 이러한 문제를 해결하기 위해서는 알고리즘의 연속동기, 순방향 오류 정정 부호 등이 사용될 수 있다.[7]

만약 CCITT V.42 모뎀이 정보보호 기능을 가지고 있다면 별도의 암호장치가 필요없고 위의 암호장치에서 해결하기 어려운 문제인 전송로상의 오류발생에 대한 보호대책도 요구되지 않으면서 정보보호 기능을 효율적으로 수행할 수 있으며 DTE간에 안전한 데이타 통신을 수행할 수 있게 해 준다.[8] 또한 CCITT에서는 V.42 모뎀에 대한 정보보호 기능 추가에 대하여 앞으로의 연구 과제로 남겨 두고 있다.

본 논문에서는 CCITT V.42 bis 구조에 대하여 검토하고 이러한 세가지 기능 즉, 오류정정 기능, 데이타 압축기능 및 정보보호 기능을 모두 만족하는 새로운 모뎀의 구조를 제안하였고, 제안한 모뎀의 기능및 서비스 프리미티브를 정의하였다. 또한 정보보호 기능의 동작과 모뎀간의 동작 절차를 서비스 프리미티브를 중심으로 상세히 기술하였다.

Ⅱ. 모뎀의 새로운 구조

1. 구 조

V.42 bis 모뎀은 V.24 접속회로(V.24 Interchange Circuits), 신호변환기(Signal Converter), 모뎀 제어기능(Modem Control Function), 오류제어기능(Error Control Function), 및 압축기능(Compression Function)으로 구성되어 있으며 그림 2와 같다.

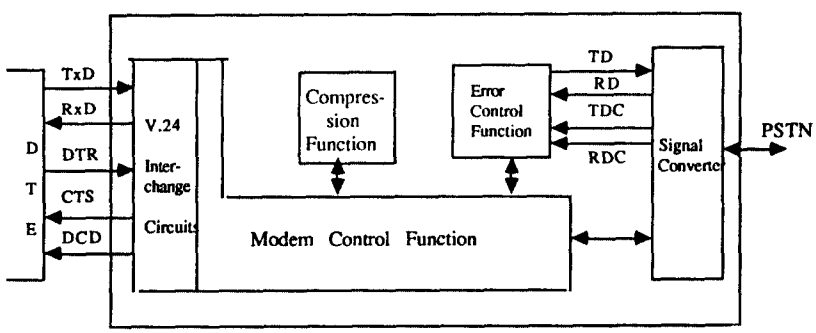


그림 2. V.42 bis 모뎀의 구조
Fig. 2. Architecture of V.42 bis modem

V.42 bis 모뎀은 압축기능과 오류제어 기능이 모뎀 제어 기능에 병렬로 연결되어 있다. 따라서 V.42 모뎀의 모뎀 제어기능은 데이타 압축을 위해서 부가적인 기능을 가져야한다.

만약 정보보호 기능이 병렬로 접속된다면 모뎀제어 기능은 정보보호 기능을 위해서 부가적인 기능을 가져야 한다.

따라서 다기능을 갖는 모뎀은 각 기능들의 독립성과 모듈화를 도모하기 위하여 직렬로 연결되는 것이 바람직하다. 또한 모뎀의 데이타 압축효율을 유지하기위해서 정보보호 기능은 압축기능과 오류제어기능 사이에 두는 것이 바람직하며 만약 압축기능이 정보보호 기능 뒤에 위치하면 데이타 압축효율은 저하될 것이다. 따라서 본 논문에서는 오류제어기능, 데이타 압축기능 및 정보보호 기능을 갖는 모뎀의 구조를 그림 3과 같이 제안하였다.

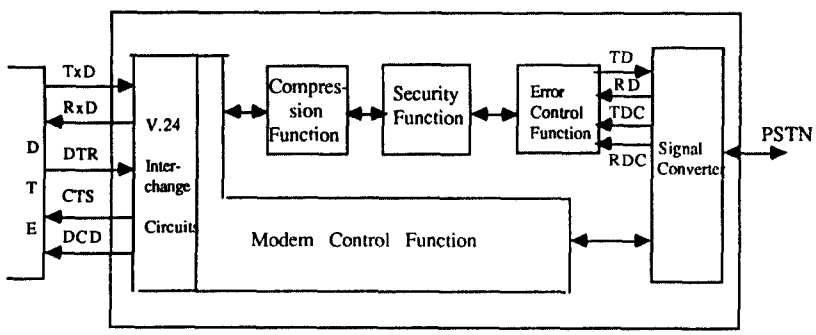


그림 3. 제안된 모뎀의 구조
Fig. 3. Architecture of the proposed modem

2. 기 능

본 논문에서 제안한 모뎀의 각 기능별 수행하여야 할 주요 동작기능은 다음과 같다.

1)모뎀 제어 기능(Modem Control Function)

모뎀 제어 기능은 초기에 특정한 신호를 주고 받음으로써 상대 모뎀이 V.42 오류 제어 기능을 가지고 있는지의 여부를 결정하고, 각종 필요한 변수와 선택적 절차의 협의를 전반적으로 조정(overall coordination)한다.

또한 물리적 접속을 수행하고 통신 링크 접속을 설정한 후 루프백 시험을 수행한다. 모뎀제어 기능은 V.24 접속회로와 압축 기능간의 사용자 데이타를 전달하고 데이타의 손실을 방지하기 위해 DTE와 모뎀 간의 흐름 제어(flow control)를 수행한다. 또한 DTE로부터 수신한 비동기 데이타를 동기 데이타로 변환하고 원격 모뎀으로부터 수신한 동기 데이타를 비동기 데이타로 변환하여 DTE로 전달한다.

2)오류 제어 기능(Error Control Function)

오류제어 기능은 V.42의 LAPM 프로토콜을 수행하며 LAPM에 관련된 변수와 선택적 절차를 협의(negotiation)한다. 오류 정정 접속후 이 기능은 LAPM 프로토콜에 따라 프레임 순서제어, 오류 검출 및 정정을 수행함으로써 전송로상에 발생되는 오류로부터 모뎀간의 오류없는 데이타 전송을 수행한다. 또한 이 기능은 모뎀간의 흐름제어 기능을 수행하고, 오류 정정 접속의 설정 및 해제를 수행한다.

3)데이타 압축 기능(Data Compression Function)

데이타 압축 기능은 상대 모뎀에 압축기능의 존재여부를 결정하고 데이타 압축 동작과 관련된 변수를 협의한다. 이러한 협의가 완료되면 데이타 압축 기능은 CCITT V.42 bis에 있는 압축 절차를 수행하며 전송 데이타를 압축하게 된다.

이기능의 주요 동작 기능으로서는 데이타 압축기능의 초기화, 데이타 압축 코딩및 디코딩, 압축 모드와 투명(transparent) 모드의 절체 기능 등이 있다.

4)정보보호 기능(Security Function)

정보보호 기능은 보안 매개변수를 협의하고 보안 접속(security connection)을 설정한다. 보안 접속후 정보보호 기능은 암호 알고리즘의 동기를 맞추기 위해 세션키를 발생하여 전달하고, 전송될 시험패턴 데

이타와 모든 사용자 데이타를 선택된 암호 알고리즘에 의해서 암호화 하고 복호화 한다.

3. 서비스 정의

V.42 bis 모뎀은 병렬 접속 구조를 가지고 있기 때문에 V.42 bis의 서비스 정의는 V.42와 관계가 적다. 예를들면 데이타 전달 서비스를 수행하기 위해서 V.42에서는 L-DATA 서비스 프리미티브를 사용하고 있는데 반하여 V.42 bis에서는 C-DATA와 C-TRANSFER 서비스 프리미티브를 사용하고 있다. 이것은 국제 표준 기구인 ISO의 서비스 프리미티브 정책에 맞지 않으므로 새로운 모뎀의 서비스 프리미티브는 ISO 정책에 따르는 것이 바람직하고, 또한 V.42에의 투명성이 요구된다.

따라서, 본 논문에서 제안한 모뎀의 서비스는 표 1과 같이 정의하였다. 서비스 프리미티브(primitive)는 요구(request), 표시(indication), 응답(response), 확인(confirm)의 네가지 형태가 있다.

제안한 모뎀의 서비스는 확인형(confirmed type)과 비확인형(unconfirmed type) 서비스로 구분하였으며, 확인형 서비스는 위의 네가지 서비스 프리미티브를 가지고, 비확인형 서비스는 요구 프리미티브와 표시 프리미티브 두가지만을 갖는다.

이와같은 구조를 가짐으로서 제안된 모뎀은 오류 정정 기능, 데이타 압축기능, 정보보호 기능을 효율적으로 수행할 수 있고 각 기능의 독립성을 유지하며, V.42에 투명하게 된다.

제안된 모뎀은 V.42에 근거한 오류 정정 기능과 V.42 bis에 근거한 데이타 압축기능 뿐만 아니라 데이타 기밀성의 보안 서비스를 효율적으로 제공할 수 있다.

표 1. 서비스 프리미티브
Table 1. Service primitives

서비스	MF〈-->$CF_{1)}$	CF〈-->$SF_{2)}$	SF〈-->$EF_{2)}$	형태
접속 설정	L-ESTABLISH	C-ESTABLISH	S-ESTABLISH	확인형
데이타 전달	L-DATA	C-DATA	S-DATA	비확인형
접속 해제	L-RELEASE	C-RELEASE	S-RELEASE	비확인형
제동신호 전달	L-SIGNAL	C-SIGNAL	S-SIGNAL	확인형
매개변수 및 선택절차협의	L-SETPARM	C-SETPARM	S-SETPARM	확인형
루프 시험	L-TEST	C-TEST	S-TEST	비확인형

주)MF : Modem control Function, CF : Compression Function, SF : Security Function, EF : Error control Function
1)V.42에서 정의된 서비스 프리미티브 2)본 논문에서 새로이 제안됨

Ⅲ. 정보보호 기능의 세부 동작

1. 구성 요소

제안된 모뎀의 정보보호 기능은 압축 기능 접속부, 오류 제어 기능 접속부, 암호블럭, 복호블럭, 암호 알고리즘블럭 및 난수(random number) 발생부로 구성되며 그림 4와 같다.

압축 기능 접속부는 정보보호 기능과 압축기능간의 서비스 프리미티브를 송수신하고, 암호 블럭은 전송될 사용자 데이타를 암호 알고리즘을 이용하여 암호화 하고, 복호블럭은 원격 모뎀으로부터 수신한 암호 데이타를 복호하여 평문으로 재생한다. 난수 발생기는 통신 세션이 이루어질 때마다 암호 알고리즘 동기를 위한 난수를 발생한다.

2. 보안 변수 협의

보안 변수는 매개변수 및 선택 절차 협의 단계에서 정보보호 기능 간에 협의된다. 보안 변수로는 데이타 암호 요구/확인, 알고리즘 식별자 및 초기 세션 키(key) 식별자가 있다.

보안 접속후 언제라도 S-SETPARM 요구 프리미티브를 오류 제어 기능으로 전달 함으로써 보안 변수를 변경 할 수있다. 본 논문에서 제안한 모뎀은 보안 변수를 전달하기 위해서 XID(Exchange Identification) 프레임을 이용하였고, 보안 변수를 협의하기 위한 XID 프레임 구조는 그림 5와 같다.[9]

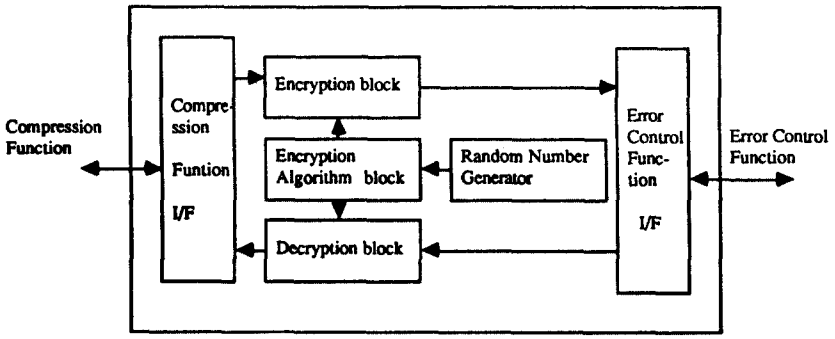


그림 4. 정보보호 기능의 블럭도
Fig. 4. Block diagram of the security function

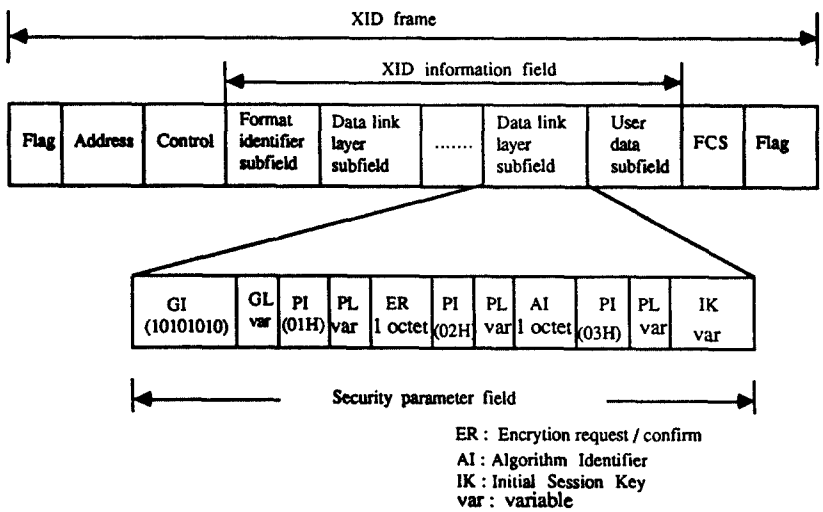


그림 5. 보안 매개변수의 협의를 위한 XID 프레임 구조
Fig. 5. Structure of an XID frame for negotiation of security parameters

XID 프레임의 정보 영역(information field)의 구조는 ISO 8885 부호화법칙에 따르며, 포맷 식별자(FI : Format Identifier), 데이타링크층 부영역(Data Link Laver Subfield) 및 사용자 데이타 부영역(User Data Subfield)으로 구성된다.[10],[11] 포맷 식별자는 1 옥텟으로 구성되며 XID 프레임의 정보 필드의 첫번째에 위치한다. 제안된 모뎀의 FI는 V.42에서와 같이 일반목적(general purpose) 포맷용으로 '10000010'으로 부호화 한다. 데이타 링크층 부영역은 다양한 데이타 링크층의 특성을 명시하기 위하여 사용되며, 1 옥텟의 그룹 식별자(GI : Group Identifier), 2 옥텟의 그룹 길이(GL : Group Length) 및 매개변수 필드로 구성되고 또한 매개변수 영역은 여러 개의 매개변수 식별자, 매개변수 길이, 매개변수 값으로 구성된다. 제안된 모뎀의 XID 프레임의 GI와 PI를 표 2와 같이 정의한다.

사용자 데이타 부영역은 사용자 데이타 식별자와 사용자 데이타 영역으로 구성된다.

표 2. 매개 변수및 선택절차 식별자
Table 2. Parameter and optional procedure identifiers

GI	PI	Parameter /Procedure
10000000	00000001	Unique Identifier
(Parameter Negotiation)	00000010	Class of procedure
	00000011	HDLC optional function
	00000101	Max.length of information field(TX direction)
	00000110	Max.length of information field(RX direction)
	00000111	Window size(TX direction)
	00001000	Window size(RX direction)
11110000	00000000	Parameter set identifier
(Compression Parameter	00000001	Data compression request(P0)
Negotiation)	00000010	Number of codewords(P1)
	00000011	Maximum string length(P2)
10101010	00000001	Data encryption request /confirm(P0)
(Security Parameter Ne-	00000010	Encrypfion algorithm identifier(P1)
gotiation)	00000011	Initial session key identifier(P2)

3. 암호화 및 복호화

정보보호 기능은 암호블럭에서 제동(break) 신호를 제외한 전송될 모든 사용자 데이타와 시험 패턴 데이타를 암호화 하고, 암호화된 데이타는 오류 제어 기능을 통하여 LAPM의 I 프레임과 시험 프레임을 통하여 전송된다. 암호 데이타를 전달하는 I 프레임과 시험 프레임의 구조는 그림 6과 같다. I 프레임과 시험 프레임의 정보 영역은 암호 기능에 의해서 암호화된 데이타로 부호화 된다. 복호블럭은 원격 모뎀으로 부터 수신한 모든 암호 데이타를 복호화 한다. 또한 정보보호 기능은 정상적인 사용자 데이타를 전달하기전에 루프백 시험 기간 동안 시험 패턴 데이타를 암호화 및 복호화 함으로써 정보보호 기능의 정확한 동작을 확인할 수 있다.

4. 정보보호 기능의 동작

압축 기능으로부터 서비스 프리미티브를 수신하였을때 정보보호 기능의 동작은 그림 7과 같다. 압축기능은 C-SETPARM 요구 프리미티브를 수신하면 정보보호 기능은 암호 알고리즘을 선택하고, 난수(random number) 발생기로부터 세션 키를 얻어 선택된 보안변수로 S-SETPARM 요구 프리미티브를 구성하여 오류 제어 기능에 전달한다.

정보보호 기능은 또한 C-SETPARM 응답 프리미

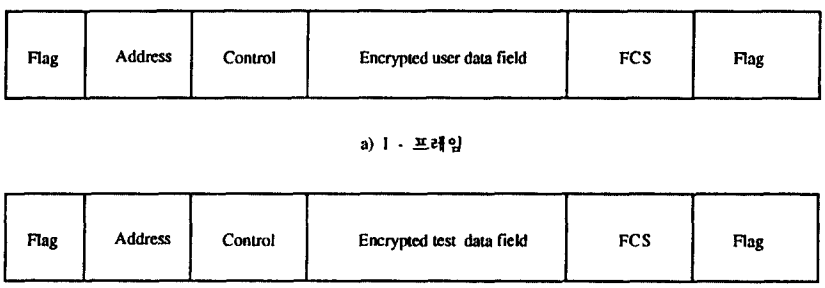


그림 6. I 프레임과 TEST 프레임의 구조
Fig. 6. Structure of an I-frame and a TEST frame

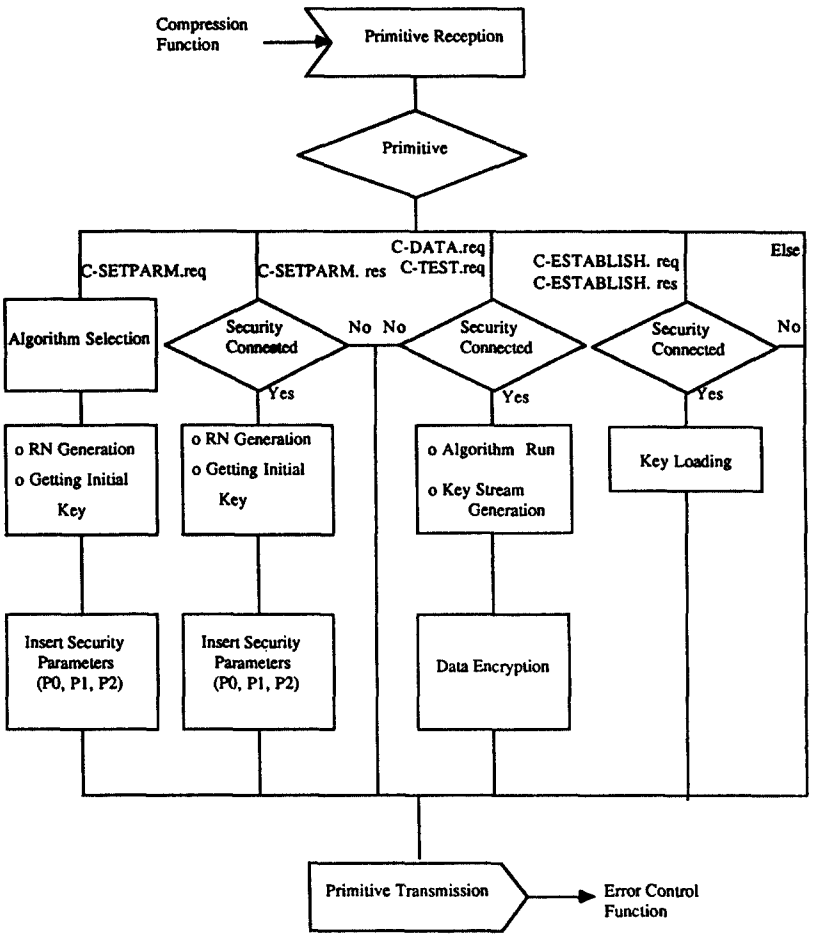


그림 7. 정보보호 기능의 송신 동작
Fig. 7. Operation of the transmitting security function

티브를 수신하면 먼저 보안 접속 상태에 있는지를 점검하고, 보안 접속 상태이면 역방향에 대해서 난수발생기로 부터 세션키를 얻고 데이타 암호확인 매개변수와 함께 보안매개변수를 삽입하여 S-SETPARM 응답 프리미티브를 오류 제어 기능에 전달한다.

통신링크 접속단계에서 C-ESTABLISH 요구 혹은 C-ESTABLISH 응답 프리미티브를 수신하면 정보보호 기능은 세션키를 선택된 암호 알고리즘에 주입한다.

정보보호 기능은 보안 접속후, C-DATA 요구 또는 C-TEST 요구 프리미티브를 수신하면 선택된 알고리즘을 이용하여 모든 사용자 데이타를 암호화 하여 S-DATA 혹은 S-TEST 요구 프리미티브를 오류 제어 기능에 전달한다. 데이타 압축 기능으로부터 수신한 그외 프리미티브들은 우회(bypass) 하도록 한다.

정보보호 기능이 오류 제어 기능으로부터 서비스 프리미티브들을 수신하였을 때 정보보호 기능의 동작은 그림 8과같다.

정보보호 기능은 S-SETPARM 표시 프리미티브를 수신하면 먼저 보안 접속이 요구되었는지를 판단하고 보안접속이 요구되었을 경우 암호 알고리즘 식별자와 세션 키를 축출하고 암호 알고리즘이 유효한지를 점검한다.

만약 알고리즘이 유효하다면, 정보보호 기능은 보

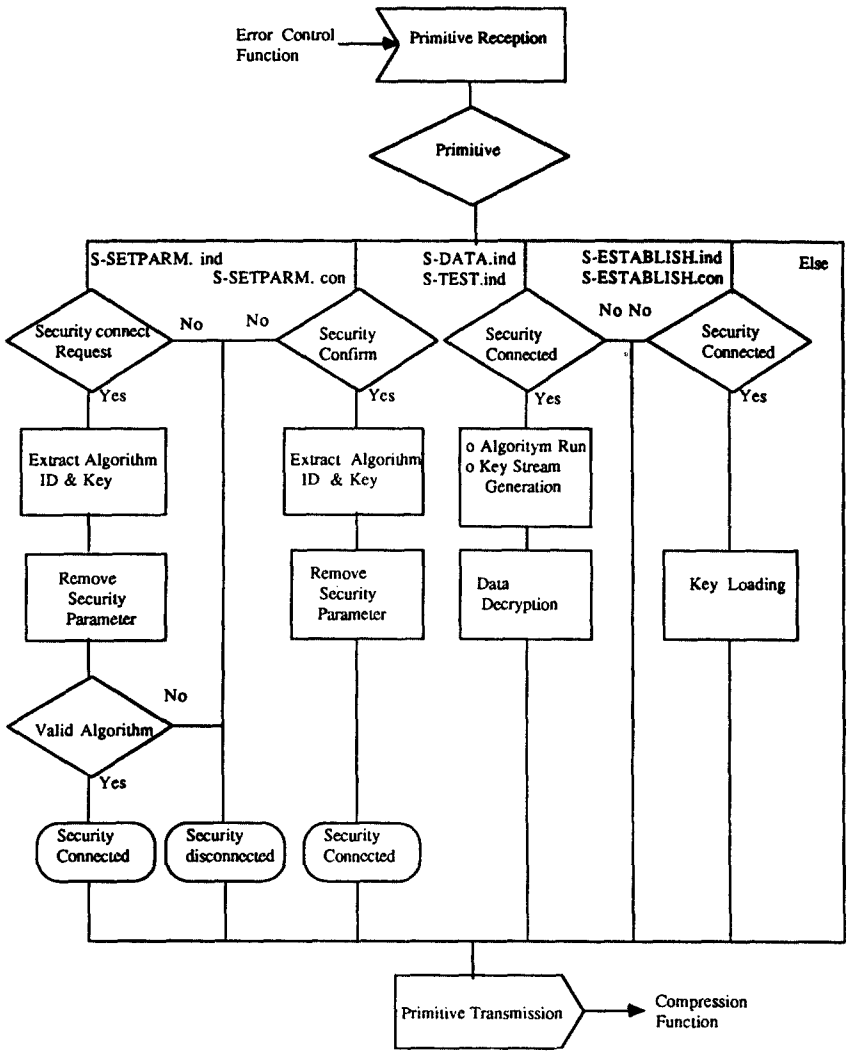


그림 8. 정보보호 기능의 수신 동작
Fig. 8. Operation of the receiving security function

안 접속(security connected) 상태로 들어가고, 유효하지 않을 경우에는 보안 미접속(security disconnected) 상태로 남게 된다. 위의 절차를 거친 다음에 정보보호 기능은 C-SETPARM 표시 프리미티브를 압축 기능에 전달한다.

정보보호 기능은 S-SETPARM 확인 프리미티브를 수신하면 보안 변수를 검사하게 된다. 만약 보안 확인 매개변수를 수신하면, 알고리즘 ID와 세션 키를 축출하고, 보안접속 상태로 변환한다. 그리고 C-SETPARM 확인 프리미티브를 압축 기능에 전달한다.

S-ESTABLISH 표시 혹은 S-ESTABLISH 확인 프리미티브를 수신하면 세션키를 선택된 암호 알고리즘에 주입한다.

보안 접속 후, S-DATA 또는 S-TEST 표시 프리미티브를 수신하면, 정보보호 기능은 모든 암호 데이타를 복호화하고, C-DATA 표시 또는 C-TEST 표시 프리미티브를 압축 기능에 전달한다.

오류 제어 기능으로부터 수신된 다른 프리미티브들은 정보보호 기능을 우회(bypass) 하도록 한다.

본 정보보호 기능에서의 암호 알고리즘은 DES (Data Encryption Standard)[12]와 같은 관용암호시스템을 사용하는 것이 바람직하며 고속 암호처리를 위해서는 암호전용 IC를 이용할 수 있다.

Ⅳ. 제안된 모뎀의 동작 절차

1. 물리적 접속 및 오류 정정 접속

제안된 모뎀의 동작 절차는 먼저 신호 변환기 간에 CCITT V 시리즈 권고에 따라 물리적 접속을 설정한 후 발신 모뎀의 모뎀제어 기능은 착신 모뎀이 오류 정정 기능을 가진 모뎀인지를 판단하기 위하여 아래와 같은 발신자 검출 패턴 ODP(Originator Detection Pattern)를 송출한다.

◦ ODP :

0 1000 1000 1 11....11 0 1000 1001 1 11....11

(우수 패리티를 갖는 DC1+8~16개의 1+기수 패리티를 갖는 DC1+8~16개의 1)

ODP를 수신한 착신 모뎀은 오류 정정 프로토콜을 수행할 수 있는지의 여부를 결정하고 그 프로토콜을 지원할 수 있는 경우에는 다음과 같은 착신자 검출 패턴 ADP(Answer Detection Pattern)-1으로 응답하고,

◦ ADP-1 :

0 1010 0010 1 11....11 0 1100 0010 1 11....11

(8~16개의 1에 의해 분리된 'E'와 'C')

만약 오류 정정 프로토콜의 지원이 불가능한 경우에는 착신 모뎀은 다음과 같은 ADP-2로 응답한다.

◦ ADP-2 :

0 1010 0010 1 11....11 0 0000 0000 1 11....11

(8~16개의 1에 의해 나누어진 'E'와 null)

이렇게 발신 모뎀과 착신 모뎀의 모뎀제어 기능간에 ODP와 ADP를 주고 받음으로써 오류 정정 접속을 설정할 수 있다.

2. 매개변수 협의

양측 모뎀간에 오류 정정 접속후 그들은 데이타 압축 매개변수 뿐만 아니라 보안 매개변수와 선택적 절차의 협의를 시작하게 된다. 그때 정보보호 기능은 상대 모뎀이 보안 접속을 설정할 수 있는지를 결정하게 되고, 또한 데이타 압축 기능은 상대 모뎀이 데이타 압축 접속이 가능한지를 판단하게 된다. 본 논문에서 제안한 모뎀간의 동작 절차는 그림 9와 같다.

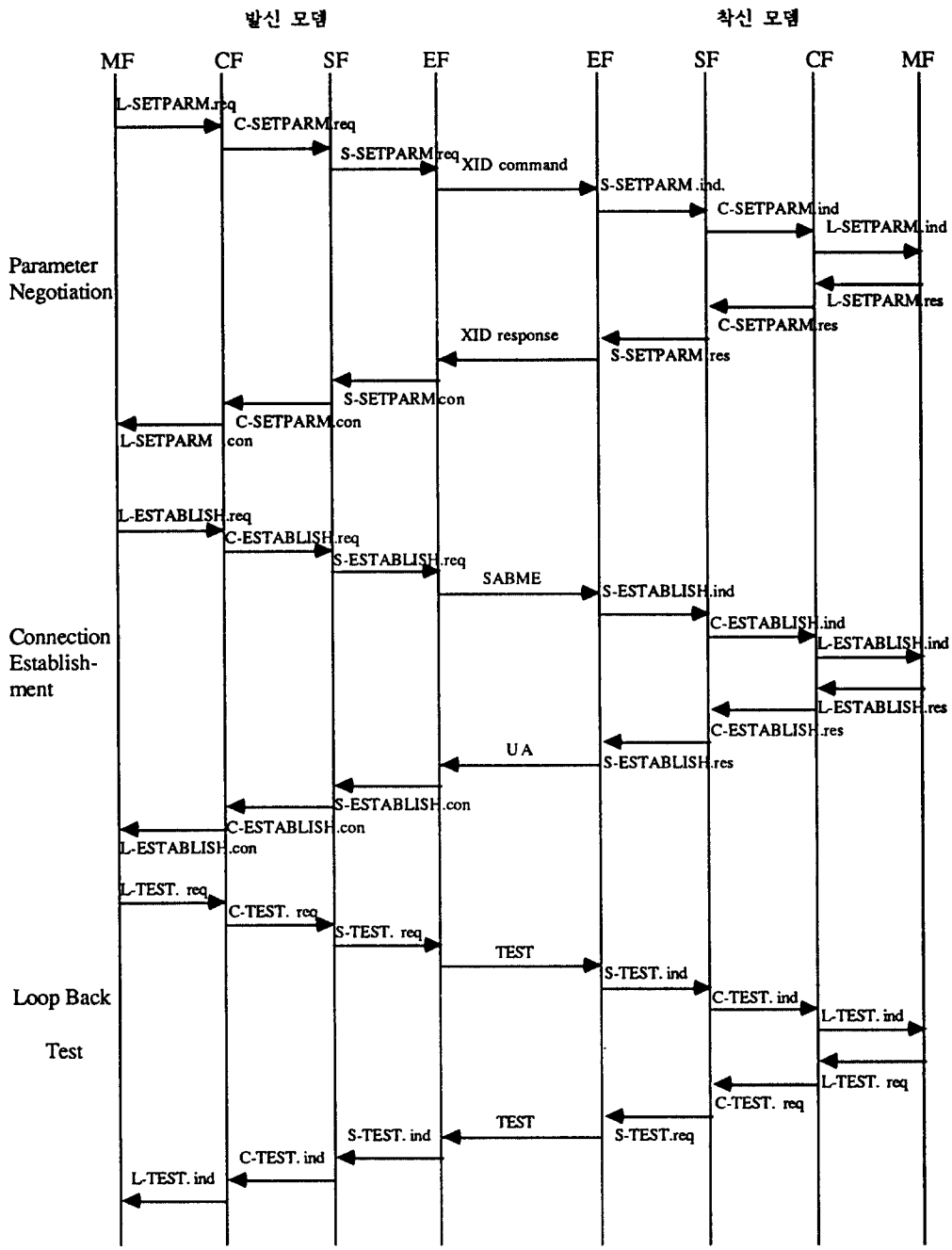
매개변수의 협의 절차는 발신모뎀의 모뎀 제어 기능에 의해서 시작되고, 정보보호 기능은 보안 매개변수들의 협의에 의해서 보안 접속을 설정하게 된다. 모뎀 제어 기능은 매개변수 협의를 위해서 L-SETPARM 요구 프리미티브를 압축 기능에 전달한다. 압축 기능은 데이타 압축 매개변수를 삽입하고 C-SETPARM 요구 프리미티브를 정보보호 기능에 전달한다. 정보보호 기능은 C-SETPARM 요구 프리미티브를 수신하면, 보안 매개변수를 추가하고 S-SETPARM 요구 프리미티브를 오류 제어 기능에 전달한다.

오류 제어 기능은 이러한 매개변수들을 XID 명령 프레임을 통하여 착신 모뎀에 전달한다. XID 명령프레임을 수신하면 착신 모뎀의 오류 제어 기능은 S-SETPARM 표시 프리미티브를 착신 모뎀의 정보보호 기능에 전달한다. 정보보호 기능은 보안 매개변수를 축출하고 C-SETPARM 표시 프리미티브를 압축 기능에 전달한다.

압축 기능은 데이타 압축 매개변수를 축출하여 L-SETPARM 표시 프리미티브를 모뎀제어 기능에 전달한다. 착신 모뎀의 모뎀 제어 기능은 응답으로서 L-SETPARM 응답 프리미티브를 압축기능에 전달한다. 압축기능은 역방향에 대해서 데이타 압축 매개변수를 삽입하고, C-SETPARM 응답 프리미티브를 정보보호 기능에 전달한다. 착신모뎀의 정보보호 기능은 보안 매개변수를 추가하여 발신 모뎀의 정보보호 기능에 응답하게 된다. 발신모뎀의 정보보호 기능은 S-SETPARM 확인 프리미티브를 수신하면 수신한 보안 매개변수를 축출하고 점검하여 보안 접속을 설정하게 된다. C-SETPARM 확인 프리미티브를 수신하면, 압축 기능은 압축 변수를 축출하고 점검한다. 매개변수 협의 절차는 발신 모뎀의 모뎀 제어 기능이 L-SETPARM 확인 프리미티브를 수신함으로써 완료 된다.

3. 접속 설정

접속 설정을 위하여 발신 모뎀의 모뎀 제어 기능은 L-ESTABLISH 요구 프리미티브를 발신하고, L-ESTABLISH 확인 프리미티브를 수신함으로써 접속 설정을 완료한다. L-ESTABLISH 표시 프리미티브를 수신하면, 착신 모뎀의 모뎀 제어 기능은 L-ESTABLISH 응답 프리미티브로 응답한다. 압축 기능



*) MF : modem control function, CF : compression function, SF : security function, EF : error control function.

그림 9-1. 제안된 모뎀간의 동작절차

Fig. 9-1. Operational procedures between the proposed modems

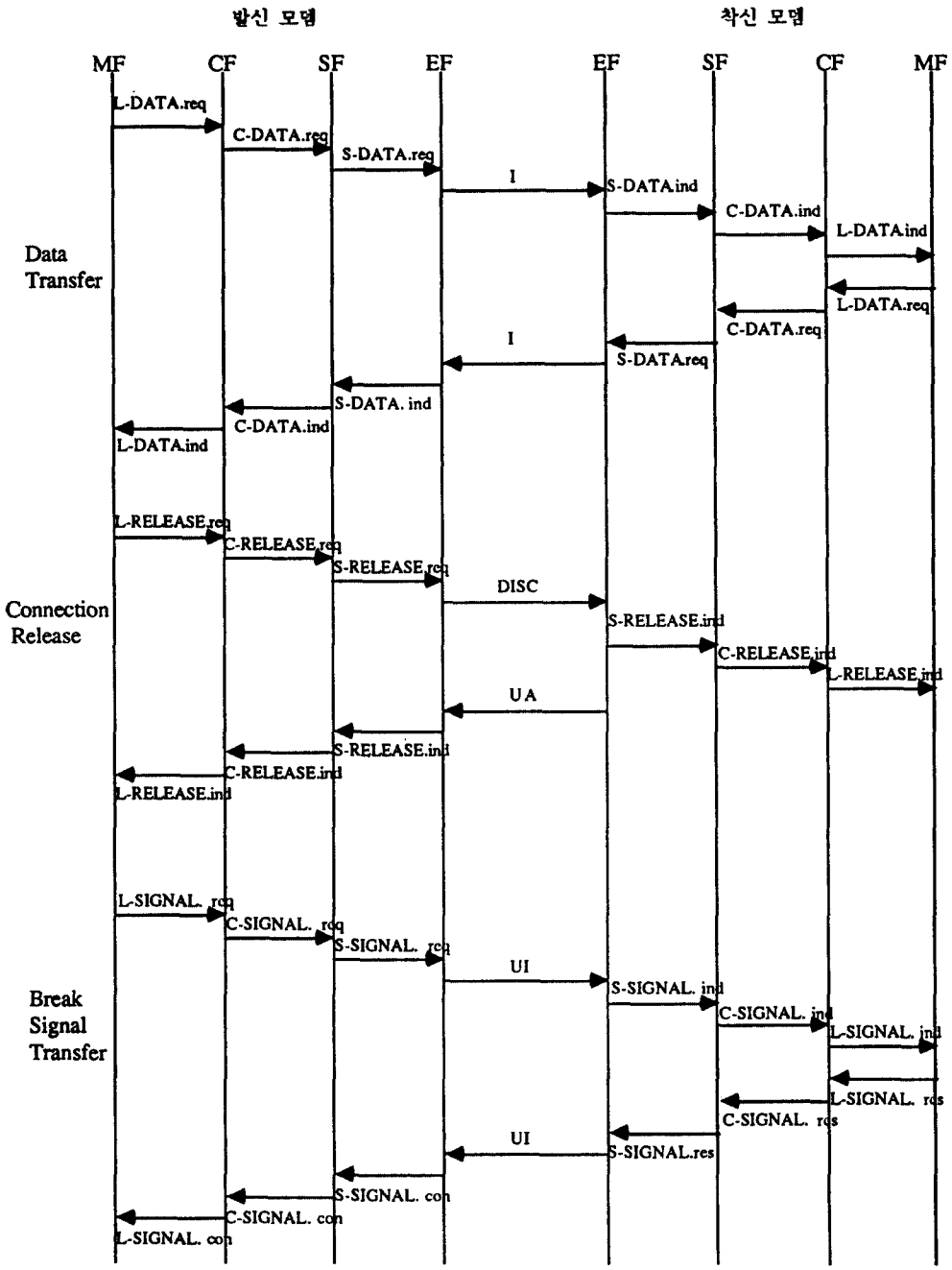


그림 9-2. 제안된 모뎀간의 동작절차

Fig. 9-2. Operational procedures between the proposed modems

이 C-ESTABLISH 표시 혹은 C-ESTABLISH 확인 프리미티브를 수신하면, 압축 기능은 부호기 및 복호기를 초기화 한다. 또한 접속설정중에 정보보호 기능은 세션키를 선택된 암호 알고리즘에 주입하여 알고리즘의 동기를 맞춘다.

4. 루프백 시험

루프백 시험을 위하여 모뎀 제어 기능은 고정된 시험 패턴 데이타를 가지고 있어야 한다. 발신 모뎀의 모뎀 제어 기능은 L-TEST 요구 프리미티브를 전송하고 압축 기능은 시험 패턴을 압축된 형태로 부호화 한다. 정보보호 기능은 압축된 시험 패턴 데이타를 암호하며 오류 제어 기능은 부호화된 데이타를 시험 프레임에 의하여 전달한다.

S-TEST 표시 프리미티브를 수신하면, 착신 모뎀에서의 정보보호 기능은 암호화된 데이타를 복호화 하고, C-TEST 표시 프리미티브를 압축 기능에 전달한다.

압축 기능에서는 C-TEST 표시 프리미티브를 수신하여 압축된 데이타를 복호화 하고 L-TEST 표시 프리미티브를 모뎀 제어 기능에 전달한다. 착신 모뎀의 모뎀 제어 기능은 수신한 데이타를 고정된 시험 패턴 데이타와 비교하여 정확한 접속동작을 확인하게 된다.

착신모뎀의 모뎀 제어 기능은 수신된 시험 데이타를 L-TEST 요구 프리미티브로 되돌려 주고 발신 모뎀의 모뎀 제어 기능은 L-TEST 표시 프리미티브를 수신하고 수신된 데이타와 송신한 시험 패턴 데이타를 비교함으로써 모뎀간의 동작을 확인 하게된다.

5. 데이타 전달

데이타를 전송하기 위해서 모뎀 제어 기능은 L-DATA 요구 프리미티브를 압축 기능으로 전달한다. 데이타 전달 단계에서 압축기능은 압축 방식에 따라 사용자 데이타를 부호화하고 수신된 압축 데이타를 복호화 한다. 한편, 정보보호 기능은 사용자 데이타를 암호화 하고 복호화 한다. 오류 제어 기능은 암호화된 데이타를 I-프레임을 이용하여 전송하고 오류 검출과 오류 정정 기능을 수행한다.

L-DATA 표시 프리미티브를 수신하면 모뎀 제어 기능은 수신된 데이타를 비동기 데이타로 변환하여 V.24 접속기를 통하여 DTE로 전달한다.

6. 접속 해제

발신 모뎀이나 착신 모뎀의 모뎀 제어 기능은 L-RELEASE 요구 프리미티브를 발송함으로써 접속을 해제 할 수 있다.

이때 정보보호 기능과 압축 기능은 그 프리미티브를 우회 시킨다. 모뎀 제어 기능은 L-RELEASE 표시 프리미티브를 수신하면 물리적 접속을 절단하고 해당 V.24 접속회로에 적절한 조치를 취한다.

7. 제동 신호 전달

압축기능이 C-SIGNAL 표시 혹은 확인 프리미티브를 수신하면 V.42 bis에서와 같이 데이타 압축기의 부호기와 복호기를 초기화 한다.

그러나 정보보호 기능은 제동 신호 전달 단계에서 그신호를 암호화 하지 않고 우회 시킨다. 제동 신호는 오류 제어 기능에서 UI(Unnumbered Information) 프레임에 의해서 전송된다. 지금까지 기술한 바와같이 제안한 모뎀은 오류 정정 서비스와 데이타 압축 서비스는 물론 암호 알고리즘을 이용한 데이타 기밀성 서비스를 효율적으로 제공할 수 있다.

V. 결 론

본 논문에서는 모뎀을 통하여 데이타 단말기간에 비동기 데이타 전송에 있어서 요구되는 오류 정정 특성, 데이타 압축특성 및 전송 데이타의 비인가적 노출에 대한 정보보호 특성을 모두 만족하는 모뎀의 구조를 제안하고, 각 기능별 동작, 서비스 정의 및 모뎀간의 동작 절차를 기술 하였다.

제안된 모뎀은 모뎀 제어 기능, 오류 제어 기능, 압축 기능과 정보보호 기능의 네가지 주요 기능으로 구성되어 있다. 이 모뎀은 전송로상의 오류 발생에 대한 오류 검출 및 오류 정정 기능을 가지고 있을 뿐만 아니라 정보보호 기능을 데이타 압축 기능과 오류 제어 기능 사이에 위치함으로써 데이타 전송 효율을 높이고 데이타 기밀성의 보안 서비스를 효율적으로 제공할 수 있도록 하였다.

정보보호 기능에 대해서는 보안 변수를 새로이 정의하였고 보안 변수의 협의에 의해서 보안 접속을 설정할 수 있으며 이러한 보안 변수들의 전달은 XID 프레임을 이용하였다.

또한 제안한 모뎀간의 상세 동작 절차를 신호 흐름도에 의해 나타냄으로써 실제 동작의 가능성을 보였으며 제안된 모뎀은 위의 기능을 갖지 않는 일반 상용 모뎀과도 접속 동작이 가능하도록 하였다.

본연구의 결과는 새로운 모뎀 개발에 적용될 수 있으며, 비동기 데이타 전송에 있어서의 정보보호 시스템 개발에 효과적으로 활용 될 수 있을 것으로 기대되며, 향후 제안된 모뎀의 효과적인 키 관리 방식에 관한 연구가 요구된다.

참 고 문 헌

1. CCITT Recommendation V.42, Error-correcting procedures for DCEs using Asynchronous-to-synchronous conversion, 1988.
2. CCITT Recommendation V.42 bis, Data compression procedures for DCEs using error correcting procedures, 1989.
3. R.J.McEliece, "A Public-Key Cryptosystem Based on Algebraic Coding Theory," DSN Progress Report Jet Propulsion Lab., Ca., pp.42-44, Jan.&Feb. 1978.
4. T.R.N. Rao and K.H.Nam, "Private-Key Algebraic-Coded Cryptosytem," Advances in Cryptology-Crypto '87.
5. Chang S. Park and Kenneth K. Tzeng, "Error-Control Private-Key Cryptosystem Based on a Concatenated Coding Scheme," proceedings of World Conference on Information Processing in Seoul, pp.150-152, 1989.
6. J.W. Chung and C.S.Wu, "The Concatenation of Compression and Secrecy Coding Schemes in the Real Time Communication Environment," Journal of the KISS, Vol.17, No.6, pp. 698-709, Nov.1990.
7. C.G.Kang and S.J.Park, "A Study on Error Evaluation and Error Performance Improvement Scheme for Stream Cipher System in Asynchronous Communication Network," WISC '89 proceedings, Vol.1, Aug.1989.
8. C.G.Kang and D.Y.Kim, "A Study on the Secure Modem," JCCI '91, Vol.1, pp.59-63, April 1991.
9. ISO 3309, Data communication-High-level Data Link Control procedures-frame structure.
10. ISO 4335, Data communication-High-level Data Link Control-Elements of procedures.
11. ISO 8885, Data communication-High-level Data Link Control procedures-General purpose XID frame information field content and format.
12. Data Encryption Standard, Federal Information Processing Standard (FIPS) Publication 46, National Bureau of Standards, U.S. Dept. of Commerce, Jan. 1977.

姜 昌 求(Chang Goo Kang) 정회원
1957년 3월 1일생
1979년 2월 : 한국항공대학 항공전자공학과졸업(공학사)
1986년 2월 : 충남대학교 대학원 전자공학과(공학석사)
1990년 3월 ~ 현재 : 충남대학교 대학원 전자공학과 박사과정 재학중
1979년 ~ 1982년 : 한국공군 기술장교
현재 : 한국전자통신연구소 선임 연구원

曺 洪 根(Hong Keun Cho) 정회원
1952년 10월 3일생
1975년 2월 : 한국항공대학 정보통신공학과졸업(공학사)
1992년 8월 : 충남대학교 대학원 전자공학과(공학석사)
1979년 8월 ~ 현재 : 한국전력공사 기술연구원 선임연구원

金 大 榮(Dae Young Kim) 정회원
1952년 5월 28일생
1975년 2월 : 서울대학교 공과대학 전자공학과(B.S)
1977년 2월 : KAIST 전기 및 전자공학과(M.S)
1983년 2월 : KAIST 전기 및 전자공학과(Ph.D)
1978년 ~ 1981년 : 서독 RWTH Aachen, UNI Hannover 공대 연구원
1987년 ~ 1988년 : 미국 University of California Davis 분교 객원연구원
1983년 ~ 현재 : 충남대학교 전자공학과 부교수