한국통신학회 1983년도 추계학술발표회 논문집 (1983· 10· 29)

컴퓨터 통신망의 DATA ENCRIPTION

83336

원 태 연
* 한국상역 컴퓨터(주)

구 고 성
* 한국 데이타통신(주)

DATA ENCRIPTION IN COMPUTER COMMUNICATION NETWORK

T. Y. WON
KIPS, KOREA

K. S. KOO
DACOM, KOREA

1. 서 론

어떠한 송신자로 부터 수신자에게 Message M 을 암호화하여 전송하는 방법은 Concealment System(1), Pravacy System(2), Secracy System 이 있다.

Secracy System 경우 Message M 은 Particular Key K 에 의해 암호화(3) $\{M\}^K$ 되어 전송되어지며 수신자측에 도달하여 풀려진다. 여기서 $\{M\}^K$ 의 비확도는 Priori Probability 의해 측정 될 수 있다.
또한 Particular Key 를 선택하여 암호화하는 Encipherer E 는 그 기능상

Simple Substitution Cipher, Transposition, Vigeneric and Variations, Matrix System, Playfair Cipher, Autokey Cipher, Fractional, Ciphers, 등등(4)

여러가지가 있을 수 있으며 Computer Network 에서 Computer 간의 암호고신은 PDN 과 같이 많은 정보를 많은 USER 에게 Service 하는경우 관심이 되어있으며 그에대한 연구가 활성화되고 있다.

Computer 경우 전송정보를 암호화하는데 특수H/W 를 부착하는 경우는 각 Line 간에 필요하므로 사용하기 어렵다. 여기서 S/W 적인 Crptographic Technique(5) 로서 같은 Domain 에 속해있는 Computer 간의 암호전송을 고찰하여 Communication Protocol 에 의한 제한점을 풀고 이에대한 이론적 배경을 고찰하여 보겠다.

2. 본 론

(정의 1) 1 Domain 속에 속해있는 Computer 와 Computer는 Complete Network 을 구성하고 있으며 Transmitter Tn 과 Receiver R 사이의 Path는 P_T^R 라 정의한다.

(정의 2) Path P_T^R 가 어떤 Communication Node A,B를 경유할 때 $P_T^R(A,B)$ 라 정의한다.

(정의 3) Particular Key K 의 INVERSE Key를 K^{-1}라 약속한다.

(정리 1) Transmitter와 Receiver 가 각기 K, K^{-1} Key value를 갖고있다면

$$K \quad K^{-1} = 1$$

이 된다.

(정의 4) Message M 은 Particular Key Value K 에 의해 Pseduo-Random-Number 의한 암호화가 된다.

$$M^1 = \{M\}^{K \bmod P}$$

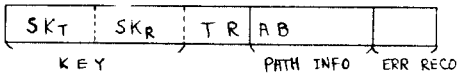
$$Ki = K_{i-1} \bmod P$$

(정의 5) Public Key 와 Security Key 를 각기 PK, SK 라 정의한다.

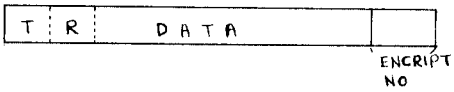
(정의 6) Initial Handshaking 이 T 와 R 사이에 일어날 경우 R, T 는 각기 Path 에 대한 Route P_T^R (A,B,.... n) 을 알 수 있다.

(정의 7) R, T간의 Polling Code 는 다음과 같다.

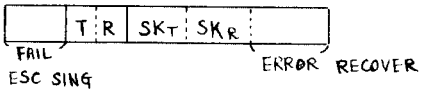
INT Poll ;



DATA POLL ;



FAIL RECOVER ;



(정의 8) P_T^R (A,B,.....N) 에서 Particular Key Ka, Kb,..Kn 은 다음과 같은 관계를 갖는다.

Ka. Kb = 1

Ka = Kb^{-1}

최초 T 와 R 간의 Communication 이 P(A, B) 를 통해 일어날 때

a. Initial

T → A : $\{K, SKt\}^{SKt}$

A → B : $\{K^{-1}, SKt\}^{Pk}$

B → R : $\{K^{-1}\ SKt, SKr\}^{SKr}$

B → A : $\{K^{-1}\ SKt, SKr\}^{Pk}$

A → T : $\{K, SKt, SKr\}^{SKt}$

b. DATA FLOW

KK = K *SKt*SKr

T → A = $\{M\}^{KK}$

A → B = $\{M\}^{KK-1}$

B → R = $\{M\}^{KK}$

이러한 Sequence 로서 P_T^R 사이의 어떤 Node 이건 최소의 Pk 만을 가지고 있으면 한 Domain 속에 속해있는 어떤 P_T^R 도 연결할 수 있으며 T,R 간에 일어나는 Encriptor 가 사용하는 Particular KK 와 SKt,SKr,Pk 는 Random Key K 와 연결되기 때문에 그 Function 을 알지않는 이상 전혀 무관하며 KK 가 Random Number Generator 외한 수일 경우 $K\ K^{-1}$ 또한 Random Number 가 된다.

(정리 2) P_T^R (A,B,.....N) 의 어떤 Network 에서 Error 가 일어나도 Routing 문제만 해결하면 Recover 가능하다.

1) A 에서 Failure 가 일어났을 경우

KKa = KKc = ... (정의 8)

고로 KK 를 알고있으니 Recover 가능하다.

2) B 에서 Failure 가 일어났을경우 1)과 같은 방법으로 가능

각 Node 에서는 Security Key 만을 가짐으로서 Table을 최소화 할 수 있으며 T,R 간의 Initial Connection 시 Message 고환을 줄일 수 있다.

(정리 3) KK 는 ModP 의 Random Cycle 을 갖는다. (정의4)를 갖고

Ki-1=K*SKt*SKr 하게하면 가능

(정의 4) Transation Over Head 는 다음과 같다.

$$\text{Transation Over Head (\%)} = \frac{\text{DATA}}{\left(\frac{\text{INT Poll Length}}{\text{DATA Poll Length}}\right) + \text{DATA}} \times 100$$

이때 최초 Handshaking 이 일어난 다음 무한히 계속된다면

$$\text{T O H} = \frac{\text{DATA}}{\text{DATA POLL LENGTH}} \times 100$$

가 될 수 있다.

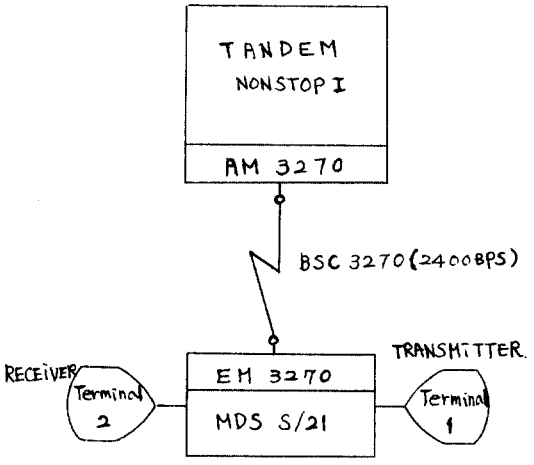
이러한 TOH 는 복잡한 PDN 의 경우 에는 Line Efficency를 올리는 것으로 상세 가능하다. 그 이유는 최초 Handshaking 시 Poll Code 의 Routing Information을 이용하여 효과적인 Path 를 제공할 수 있기 때문이다.

이에대한 Algorithm 은 다음과 같다.

START : Get Random K Value
Make $\{K, SKt\}^{SKt}$
Send Init Poll M to A
Get Message M From A
If SKt in M
then GO TO Message
else GO TO START

MESSAGE : MAKE Message M TO $\{M\}^{KK}$
SEND $\{M\}^{KK}$ TO A
IF ESC ERROR IN M FROM A
THEN GO TO COVER
ELSE GO TO MESSAGE
COVER : GET KK IN M
GO TO MESSAGE

이러한 이론을 배경으로 다음과 같이 Test 하였다.



Encriptor 의 Parameter 는 다음과 같다.

K = 32

SKt = 62231

SKr = 67235

KKi = KKi-1 *75637 (Mod 2^{31})

3. 결 론

이 논문은 Computer Network 상에서

(1) Key Value 를 줄이고

(2) Network 상의 Key Value를 Inverse Value 를 빼함으로서 Network Failure 시 Recover 용이

(3) Routing 문제의 해결에 도움을 주는 방법을 제시하였다.

그러나 어떠한 이론이나 Test 에도 완전한 것은 없는 것이니 더욱 복잡하고 많은 user 에게 무한한 비확도를 갖는 방법에 대한 연구가 계속되어야 할 것이다.

((참 고 문 헌))

1. Probability, Random Variable and Stochastic Processes - Papoulis
2. System Simulation - Geoffrey Gordon
3. Pathway - TANDEM
4. EM3270 PHASE II - Mohawk Data Science
5. Encryption and Authentication in On-Board Processing Satellite Communication System - IEEE : Communication Nov 81
6. Digital Signature Schemes for Computer Communication Networks
7. Using Encryption for Authentication in Large Networks of Computer - ACM Dec 1978 P996-999
8. Multiuser Cryptographic Techniques - National Computer Conference 1976
9. An Improved Algorthm for Computing Logarithms over GF(P) and its Cryptographic Significance - IEEE INFORMATION Theory Jan 1978 P106-110
10. Encription and Ensure Computer Networks - Computer Survey Dec 1979
11. Some Cyptographic Techniques for Machine to Machine Data Communication - Proceding OF IEEE Nov 1975 P1545-1554
12. Communication Theory of Secrecy Systems - Shannon