무선 통신망 암호동기에 적합한 Statistical CFB 방식의 암호 알고리즘 성능 분석

박대선* · 김동수* · 김영수* · 윤장홍*

Performance Analysis of a Statistical CFB Encryption Algorithm for Cryptographic Synchronization Method in the Wireless Communication Networks

Dae-seon Park* · Dong-soo Kim* · Young-soo Kim* · Jang-hong Yoon*

요 약

본 논문에서는 통신 채널의 오류로 인하여 통신 단말 간에 서로 송수신되는 정보중에 임의의 비트가 삭제되거나 추가되어 암호 알고리즘을 사용하여 통신이 불가능해지는 경우, 이를 극복하기 위한 기법으로 Statistical CFB 방식의 암호 알고리즘을 제안한다. 먼저, 비트 삽입 또는 비트 삭제 발생 시 오류 전파의 영향을 수학적으로 모델링하여 이론적인 Statistical CFB 암호 알고리즘의 성능을 분석한다. 이 경우, Statistical CFB 방식의 성능을 결정하는 요소인 동기 패턴의 길이와 피드백되는 키의 길이를 변화해가며 분석하도록 한다. 또한 이론적인 분석과 함께 실제로 특정 길이의 동기 패턴과 피드백되는 키를 선택한 후, Statistical CFB 방식을 적용한 암호 알고리즘을 사용하여 성능을 분석하였다. 이를 이론적인 분석 결과와 비교하여 제안된 암호 알고리즘의 타당성을 검증한다.

ABSTRACT

This paper suggests a new cipher mode of operation which can recover cryptographic synchronization. First, we study the typical cipher modes of operation, especially focused on cryptographic synchronization problems. Then, we suggest a statistical cipher-feedback mode of operation. We define the error sources mathmatically and simulate propagation errors caused by a bit insertion or bit deletion. In the simulation, we compare the effects of changing the synchronization pattern length and feedback key length. After that, we analyze the simulation results with the calculated propagation errors. Finally, we evaluate the performance of the statistical cipher-feedback mode of operation and recommand the implementation considerations.

키워드

Cryptographic Synchronization, Cipher Modes of Operation, Channel Errors, Statistical CFB

Ⅰ. 서 론

암호 알고리즘을 사용하여 정보보호 서비스를 제공하고자 하는 경우, 암호 알고리즘의 동작 방식은 실제로 보안 레벨을 결정하는 동시에 암호 통신의 품질을 크게 좌우하게 된다. 특히, 무선 통신망의 경우 송수신 단말간의 통신 채널의 품질이 열악한 환경하에서는 통신 채널의 에러가 암호 통신을 하는데 매우 큰 영향을

* 국가보안기술연구소

접수일자 : 2005. 8. 12

발생하게 된다. 이중에서도 비트의 삽입 또는 비트의 삭제와 같은 통신 에러는 암호 통신 시 동기의 이탈을 발생시킬 수 있으며 결과적으로 통신 불능 상태의 주된 원인이 될 수 있다. 따라서, 이와 같은 열악한 통신 채널 환경에서 암호 알고리즘을 사용하여 암호 통신 동기를 유지할 수 있는 효과적인 암호 알고리즘 동작 방식이 요구된다.

본 논문에서는 암호 통신 시 발생되는 암호 동기 문제를 극복하기 위한 기법으로 Statistical CFB 방식의 암호 알고리즘을 제안하였다[2][4][5]. 기존 암호 알고리즘의 동작 방식 적용 시 동기 복구가 불가능한 원인에 대해서 간략하게 검토하고 제안된 암호 알고리즘의 동작 방식에 대해서 설명하였다. 또한, 에러의 종류를 구분하고 모의 실험을 통하여 그 결과를 분석하였으며 실제로 구현된 Statistical CFB 방식의 암호 알고리즘을 사용하여 암호 통신 시 성능을 분석하였다.

Ⅱ. 기존 운영방식의 고찰

다양한 통신 채널 환경에서 암호 알고리즘을 적용하여 암호 통신 동기를 유지하고자 하는 경우, 현재 보편적으로 사용되고 있는 알고리즘 운영 방식에 대하여 신중히 검토해 볼 필요가 있다.

먼저, ECB 방식은 주어진 평문을 n비트씩 나누어서 차례로 암호화하는 방식이다[1][3]. 단순한 비트 에러 발생 시에는 에러가 해당 복호문에만 영향을 미치게 되지만 랜덤 비트 에러가 발생하는 경우에는 비트 수에 관계없이 모든 비트에서 1/2의 확률로 에러가 발생하는 단점이 있다[1].

CBC 방식의 경우 비트가 변경되는 에러에 대해서는 자동적으로 동기가 맞추어지지만 비트의 삽입이나 삭제로부터 발생되는 에러에 대해서는 동기를 회복하는 것이 불가능하다.

CFB 방식을 사용하는 경우 암호문의 비트가 바뀌는 경우에 대해서는 블록 사이즈를 n, 피드백되는 비트 사이즈 r이라 하면 [(n/r)+1]개의 암호문 이후에 자동으로 동기가 맞추어진다. 하지만 이 방식 역시 임의의 비트가 삽입되거나 삭제되는 경우 동기 회복이 불가능하다.

마지막으로 OFB 방식은 단순한 비트 에러는 암호문에 대응되는 복호문에서 특정 비트 에러로 나타난다. 하지만 암호문에 에러가 발생한 경우 수신측에서는 이를 탐지할 수 없으므로 별도의 방법을 사용하여 수시로 동기를 맞추어 주어야 한다.

Ⅲ. Statistical CFB 운영 방식

1. 알고리즘의 기본 개념

Statistical CFB 방식은 그림 1과 같이 초기 암호화 키를 사용하여 암호문을 생성하게 된다.

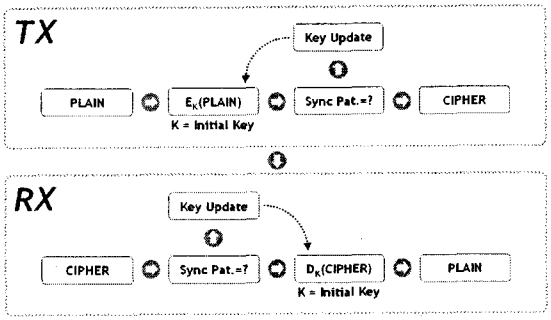


그림 1. Statistical CFB의 개념
Fig. 1 Concept of the Statistical CFB

암호화된 암호문 내의 특정 비트들의 패턴을 인식하여 이 패턴이 탐지된 경우 특정 패턴 이후 임의의 길이 만큼의 암호문을 다음 암호문을 생성하기 위한 키로 피드백하여 사용한다.[2][4][5][6]

이때, 암호문 내의 특정 패턴 정보를 '동기 패턴(Sync Pattern)'이라고 정의하며 이러한 동기 패턴은 수신측에서 동일하게 정의하여 사용한다.

암호화 키 이후 다시 동기 패턴이 나오기 전까지의 데이터들은 현재의 암호화 키로 암호화 및 복호화를 한다. 다시 동기 패턴이 탐지되었을 경우 이전의 암호화 키는 버리고 암호화 키를 새로 업데이트 한다.

2. 에러 유형의 분류 및 영향 분석

2.1. 에러 유형의 분류

2.1.1. 패턴 손실 에러

이 경우 전송 선로의 에러로 인하여 송신측의 8비트 동기 패턴에 에러가 발생하면, 수신측에서는 이를 동기 패턴으로 인식할 수 없게 되므로 에러가 발생하게 된다.

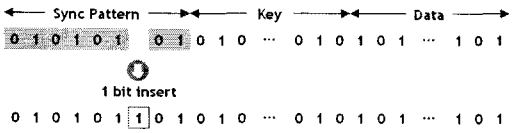


그림 2. 패턴 손실 에러
Fig. 2 Pattern Missing Error

따라서, 이러한 Pattern Missing의 경우에 대해 모의 실험 프로그램의 알고리즘은 송신측의 몇 번째 동기 패턴이 수신측에 일반 암호문으로 전달되었는지를 탐지하고 이를 에러로 계산하여 전체 시스템의 에러에 포함한다.

2.1.2. 패턴 오판 에러

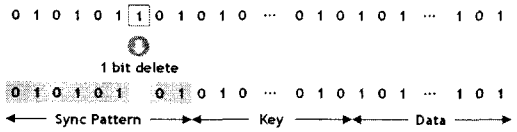


그림 3. 패턴 오판 에러
Fig. 3 False Detection Error

송신측에서 전송된 정보에 동기 패턴에 대한 어떠한 정보도 포함되어 있지 않지만, 전송 선로의 에러로 인하여 수신측에서 동기 패턴으로 인식되는 경우이다.

이렇게 전송 되지도 않은 동기 패턴을 동기 패턴으로 인식하는 경우에 대해서도 모의 실험 프로그램의 알고리즘은 암호문 데이터의 몇 번째 비트가 동기 패턴으로 인식되고 있는지 탐지를 하며, 이러한 에러를 계산하여 전체 에러 성분에 포함시킨다.

2.1.3. 피드백 키 데이터 에러

송신 및 수신 데이터의 동기 패턴에는 문제가 없고 동일한 패턴이 인식 되었지만, 송수신 각각의 암호화/복호화 키가 동일하지 않은 경우이다.

이 경우, 송신 및 수신 측 암호화/복호화 키가 동일하지 않게 되므로 수신측에서 복호화된 데이터는 원래 암호화되기 전의 데이터와 일치하지 않게 된다. 이러한 경우에 대해서도 모의 실험 프로그램 알고리즘은 몇 번째 동기 패턴 이후의 암호화/복호화 키가 일치하지 않는 지를 탐지하여 계산하고, 이를 전체 시스템 에러 성분에 포함시킨다.

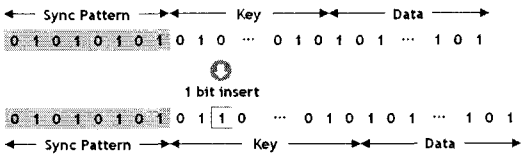


그림 4. 피드백 키 데이터 에러
Fig. 4 Feedback Key Data Error

2.2. 에러 영향 분석

먼저, 다음과 같은 파라미터를 정의한다.

- n : 동기 패턴의 비트 수
- m : 키의 비트 수
- P_b : 비트 에러율(BER)

그리고, 선로상의 에러로 인해 발생할 수 있는 에러 요인의 경우는 다음과 같이 모두 3가지로 나누어 볼 수 있으며, 전체 시스템의 에러는 이들 각각의 에러를 모두 더하여 구할 수 있다.

- 전송 키에 에러가 존재하는 경우
  (동기 패턴은 일치)
- 동기 패턴을 정확히 수신하지 못 한 경우
  (패턴 손실 에러, Pattern Missing Error)
- 동기 패턴을 잘못 인식하는 경우
  (패턴 오판 에러, False Detection Error)

위의 3가지 에러 발생 경우를 제외하고는 수신 시스템에는 전송 선로의 에러만이 존재하게 된다.

이때, 채널 BER을 P_b라고 하면 시스템의 동기 패턴에 에러가 없을 확률은 다음과 같다.

$$P_{no-errors-sync} = (1-P_b)^n \quad (1)$$

또한, 암호화 키 부분에 에러가 발생하지 않을 확률은

$$P_{no-errors-key} = (1-P_b)^m \quad (2)$$

이다. 따라서, 동기 패턴 및 암호화 키 부분에 에러가 발생할 확률은

$$P_e = \{1-(1-P_b)^{n+m}\} \quad (3)$$

이고, 이때 전체 동기 패턴이 발생하는 주기에 대해 동기 패턴 및 암호화 키 부분에 에러가 발생하는 확률은

$$P_{e1} = 0.5^* \{1-(1-P_b)^{n+m}\} \quad (4)$$

로 표현할 수 있다.

다음, 동기 패턴을 인식하지 못한는 경우의 에러를 살펴보면, 먼저 동기 패턴 및 키 부분에서 에러가 없을 확률은

$$P_e = (1-P_b)^{n+m} \quad (5)$$

와 같이 쓸 수 있다. 이때, 전송 선로의 에러에 따라 동기 패턴이나 키에 에러가 발생하므로, 시스템에서 동기 패턴을 인식하지 못하는 경우의 에러는

$$P_{e2} = \{(1-P_b)^{n+m}\}^* P_b \quad (6)$$

과 같이 쓸 수 있다.

마지막으로, 세번째 에러 요인을 식으로 표현하면

$$P_{e3} = 0.5^* \sum_{i=1}^{n} \{\frac{n!}{(n-i)!}^* (1-P_b)^{n-1}{}^* P_b^i\} \\ * \frac{2^n-(n-m)+1}{2^n-1} \quad (7)$$

와 같이 된다.

따라서, 전송 선로의 에러로 인하여 발생된 에러를 포함한 암호문으로 수신측에서 Statistical CFB 방식의 암호 알고리즘을 적용하여 암호문을 복호화하는 경우 발생되는 전체 시스템의 에러는

$$P_{total-error} = P_{e1} + P_{e2} + P_{e3} \quad (8)$$

로 나타낼 수 있다.

3. 모의 실험

3.1. 모의 실험 방법

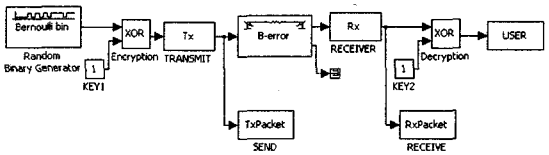


그림 5. 모의 실험 프로그램 블럭도
Fig. 5 Block Diagram of the Simulation Program

먼저, 송신 동기 패턴 정보가 수신 동기 패턴 정보와 일치하는지를 비교한다. 동기 패턴이 일치하는 경우 암호화/복호화 키를 비교하며, 이 때 키 또한 일치하는 경우에 대해서는 다음 동기 패턴이 발생 할 때까지 데이터 중의 에러를 카운트 한다. (Error1)

키가 일치하지 않는 경우 다음 동기 패턴이 발생할 때까지 시스템 에러를 계산한다. (Error2)

동기 패턴이 일치하지 않는 경우, 즉 Pattern Missing의 경우 동기 패턴 정보에 수신측에 잘못 전송된 경우 정상적인 동기 패턴이 탐지될 때 까지의 에러를 계산한다. (Error3)

False Detection의 경우, 송신측에 존재하지 않는 동기 패턴 정보를 수신측이 인식하는 경우 정상적인 동기 패턴이 탐지될 때 까지의 에러를 계산한다.

이 과정을 생성된 데이터가 끝날 때 까지 반복한다. 위의 모든 과정이 끝나면, 계산된 에러 성분(Error1부터 Error4)을 모두 더하여 전체 시스템의 에러를 계산한다.

3.2. 모의 실험 결과

그림 6에서 ①의 의미는 송신측 데이터 내의 동기 패턴의 위치를 나타낸다. ②에서는 송신측에서 전송된 데이터 내에 에러를 포함하는 경우, 송신측에서 탐지된 동기 패턴의 위치를 나타낸다.

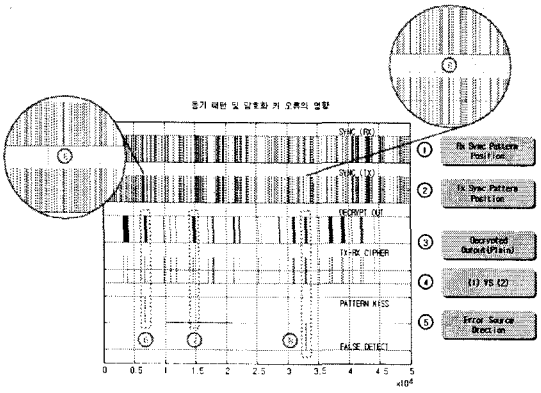


그림 6. 복호문에서 암호문 에러의 영향
Fig. 6 Error propagation result which are caused by the defined error sources

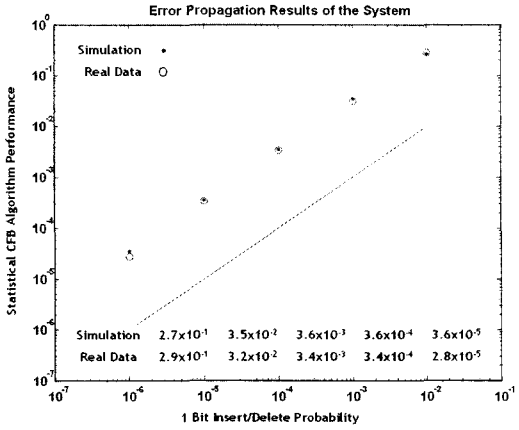


그림 7. 시스템의 에러 전파 결과
Fig. 7 Error Propagation Results of the System

③의 결과가 나타내고 있는 것은 수신된 암호문을 복호화하여 최초 송신측에서 송신한 데이터와 비교한 결과 복호화된 평문에 발생된 에러를 의미한다.

④는 에러가 포함된 수신 암호문과 송신 암호문을 비교한 결과이다. 여기서, ①과 ②의 결과를 비교하면 ⑤의 결과처럼 현재 시스템에서 몇 번째 동기 패턴에 에러로 인하여 Pattern Missing이 발생했는지, 아니면 False Detection이 발생했는지 분석이 가능하다. ⑤의 결과를 바탕으로, ③에서 발생되는 에러의 원인이 Pattern Missing, False Detection, 혹은 Key Error인지를 판단할 수 있게 된다.

⑥은 Pattern Missing이 발생한 경우로서 송신측 암호문의 동기 패턴이 수신측에서는 탐지가 되지 못하여 암호문을 복호화한 결과 ③에서처럼 에러가 검출되었다.

⑧은 ⑥의 반대로 False Detection이 발생하여 송신측에서의 일반 암호문이 수신측에서 동기 패턴으로 인식되어 ③과 같이 에러로 검출되었다.

⑦은 Pattern Missing이나 False Detection이 아닌 암호화 키의 에러로 인하여 복호화된 암호문 내에 에러가 검출되는 경우이다.

그림 7의 결과는 1Mbit의 데이터를 모의 실험 조건과 동일한 조건으로 10회 암호화/복호화를 실시하여 평균값을 취한 것이다. 실제 구현된 Statistical CFB 방식의 암호 알고리즘은 수학적으로 계산된 성능보다 우수한 결과를 나타냈다. 실제로 사용된 알고리즘의 결과는 모의실험의 결과와 비교해 보았을 때, 주어진 채널 특성에서 평균 약 7%에서 9%의 성능 향상을 나타내었다.

Ⅳ. 결 론

지금까지 Statistical CFB 방식의 암호 알고리즘의 동작 방식, 특성 및 모의 실험 결과를 실제로 시스템을 구현하여 암호화한 데이터의 분석과 함께 살펴보았다. 또한 Statistical CFB 방식의 암호 알고리즘을 적용하였을 경우 발생 가능한 에러 요인을 살펴보았으며, 이를 모의 실험 프로그램으로 구현하는 방법에 대해서도 살펴보았다. 마지막으로, 수식적으로 계산된 결과값과 모의 실험을 통해서 얻어진 결과값의 비교를 통하여 모의 실험이 올바르게 수행되었는지에 대해서도 살펴보았다.

Statistical CFB 방식의 암호 알고리즘 적용 시 동기 패턴의 길이를 너무 짧게 설정하는 경우 시스템의 동기 패턴 인식 횟수가 필요 이상으로 증가하여 시스템에 무리를 줄 수 있다. 반대로 동기 패턴의 길이를 너무 길게 설정하는 경우에는 Statistical CFB를 사용하더라도 큰 효과를 기대하기 힘들다.

따라서, Statistical CFB 방식은 열악한 통신 채널 환경에서 암호 통신 동기를 유지하기 위하여 시스템에 무리를 가하지 않으면서도 높은 안전성을 제공을 할 수 있는 동기 패턴의 길이와 키의 길이를 고려하여 설계하여야 한다.

참고문헌

[1] Morris Dworkin, NIST, "Recommendation for Block Cipher Modes of Operation", 2001

[2] Oliver Jung, "Encryption with Statistical Self Synchronization in Synchronous Broadband Network", CHES99, 1999

[3] Alfred J. Menezes, "Handbook of Applied Cryptography", CRC Press, 1997

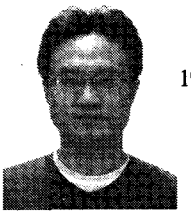
[4] Heys, H.M, "An analysis of the statistical self-synchronization of stream ciphers", INFOCOM 2001, Proceedings. IEEE Vol.2, 22-26 April 2001 pp.897-904

[5] Heys, H.M, "Analysis of the statistical cipher feedback mode of block ciphers", Computers, IEEE Transactions on Vol.52, Issue 1, Jan. 2003 pp.77-92

[6] Douglas Stinton, "Cryptography Theory and Practice", CRC Press, Inc., Second Edition, February 2002,

[7] http://cnscenter.future.co.kr/

저자소개



박대선(Dae-Seon Park)

1999년 건국대학교 전자공학과 졸업. 동 대학원 석사 (2001년). 2005년 현재 국가보안기술연구소 재직 중.

※관심분야 : 위성통신, 암호 알고리즘, 최적 제어

김동수(Dong-Soo Kim)

2005년 현재 국가보안기술연구소 재직 중.

김영수(Young-Soo Kim)

2005년 현재 국가보안기술연구소 재직 중.

윤장홍(Jang-Hong Yoon)

2005년 현재 국가보안기술연구소 재직 중.