CBC-MAC 기반의 위성 관제 신호 보호 알고리즘

준회원 곽 원 숙*, 조 정 훈*,
정회원 홍 진 근**, 박 종 욱**, 김 성 조**, 윤 장 홍**, 이 상 학***, 황 찬 식*

TT&C security algorithm of satellite based on CBC-MAC

Won-sook Kwak*, Jeong-hoon Cho* *Senior Members*, Jin-keun Hong**, Jong-wook Park**,
Sung-jo Kim**, Jang-hong Yun**, Sang-hak Lee***, Chan-sik Hwang* *Regular Members*,

요 약

인공 위성을 이용한 위성 통신망에서는 위성의 위치, 성능, 그리고 동작을 제어하는 관제신호(Telemetry, Tracking and Command, TT&C)채널의 보호가 요구된다. 본 논문에서는 관제신호의 생성 및 수행의 보안을 위하여 사용되는 인증 알고리즘의 취약점을 분석하고, 부가적인 계산량을 크게 증가시키지 않으면서도 키 복구 공격(key recovery attack)에 대해 구조적으로 보완하는 인증 알고리즘을 제안하고 검증하였다. 제안한 인증 알고리즘은 입력으로 사용되는 관제신호 데이터의 크기와 메시지 인증 코드의 크기를 변경하지 않아 기존의 위성 시스템에 그대로 적용 가능하며 키 복구 공격에 대한 계산 복잡도를 기존의 2^{55} 번의 수행에서 2^{111} 번으로 증가시켜 Rivest의 권고안을 만족시킬 수 있음을 보인다.

ABSTRACT

In satellite communication, which use the satellite, the protection of TT&C channel which controls the position, performance, and operation is required. In this thesis, we analyzed the weakness of authentication algorithm which is used for protection of TT&C generation and operation. Also, we proposed the authentication algorithm which complements key recovery attack structurely without increasing additional computational amount and verified its performance. The proposed authentication algorithm can satisfy Rivest's recommendation by increasing the computational complexity from 2^{55} operations to 2^{111} operations. In addition, it can be applied to the existing satellite system because the length of TT&C data and message authentication codes used for the input of authentication algorithm are unchanged.

I. 서 론

오늘날 사회가 다양화되고 복잡해짐에 따라 필요한 정보의 양은 급속히 증가하고 있으며 이에 부응하여 인공위성이 군사용, 과학 실험용, 통신 방송용 등 폭 넓은 분야에서 이용되고 있다. 최근에는 멀티미디어의 등장과 컴퓨터 통신, 이동 통신, 위성 방송 등을 이용하는 정보화 사회의 도래로 말미암아 정보 전달의 양이 대용량화되고 있는 추세이고 정보 전달 매체로서의 위성통신에 대한 수요가 폭증하고 있는 실정이다. 하지만, 위성통신은 유선 통신과는 달리 전송 매체로 전파를 이용하고 빔 커버리지(coverage)가 넓은 관계로 정보 보안에 대한 위협이 더욱 크다고 할 수 있다. 위성통신에서 안전성을 해치는 위협 요인은 매우 다양하며 이는 기본적으로 기존의 통신망에서 발생 가능한 위협 요인을 모

* 경북대학교 전자공학과 데이터 통신 시스템 연구실(kws0957@palgong.knu.ac.kr),
** 한국전자통신연구원 부설 국가보안기술연구소(jkhong@etri.re.kr), *** 동양대학교 정보통신 공학부(shaklee@phenix.dyu.ac.kr)
논문번호 : 020114-0313, 접수일자 : 2002년 3월 13일
※ 본 연구는 한국전자통신연구원 부설 국가보안기술연구소 연구과제 지원으로 수행되었습니다.

두 포함하고 있다. 위성통신에서 발생 가능한 위협 형태 중 사람에 의해 인위적으로 발생하는 형태는 가로채기(interception), 가로막기(interruption), 변조(modification), 위조(fabrication) 등이며 이에 대해 효과적으로 대처할 수 있는 것은 적절한 보호 기술의 적용이다. 특히 위성의 위치, 성능 및 동작을 제어하는 위성관제 신호의 보호는 매우 중요하다. 관제신호의 안전한 송수신이 이루어지지 않는다면 악의를 가진 제 3자에 의해 위성을 쉽게 탈취 당하게 되어 큰 사회적 혼란을 초래할 수 있다.

위성관제 통신은 위성의 내부 동작 상태, 위성의 위치와 동작 상태를 무선으로 원격감시 및 측정하여 이 처리결과에 따라 무선으로 원격명령을 보내어 위성을 제어하기 위해 지상 관제소와 위성간에 이루어지는 통신을 말한다. 위성관제 신호는 크게 원격명령(command), 원격측정(telemetry), 거리측정(ranging)으로 구성된다[1]-[3]. 지상 관제소는 위성으로부터 위성의 상태, 자세, 성능에 대한 정보를 가진 원격측정신호를 수신하여 위성을 추적(tracking)하고 이에 대응하는 원격명령신호를 보내어 위성을 제어한다. 원격명령신호는 위성 구성요소의 on/off 상태와 시스템 설정, 궤도 내 속도 및 위치, 지향성 유지, 탑재체 상태 등을 제어할 수 있다. 따라서, 위성으로 전송하는 원격명령신호에 대해 위성은 정당한 지상 관제소로부터 보내온 신호인지를 확인할 수 있어야 한다. 만약 위성명령신호를 정확히 인증하지 못한다면 위성은 악의를 가진 사람에 의해 이용될 수 있으므로 이에 의한 파급효과는 큰 사회적 혼란을 초래할 수 있다. 원격명령신호의 생성 및 수행의 보안을 위하여 여러 가지 방법이 사용되고 있는데, 원격명령신호를 이미 약속한 비밀키와 블록 암호 알고리즘으로 DES(Data Encryption Standard)를 이용하여 메시지 인증 코드를 생성한 후 전송하고 위성에서 인증하는 방법을 관제신호 보호 알고리즘으로 가장 널리 사용하고 있다[4].

컴퓨터의 연산 속도의 발전과 병렬 키 탐색 기계의 설계로 인하여, 최근에는 계산상 불가능의 기준이 2^{80} 이상의 계산 복잡도가 요구되는 것으로 설정되고 있다[5]. 이에 의하면 관제신호 보호 알고리즘은 DES 알고리즘을 이용한 구현으로 인해, 현재 DES에서 제기되고 있는 여러 취약점들을 내포하고 있다고 할 수 있다. 본 논문에서는 위성통신에서 사용되고 있는 원격명령신호 보호 알고리즘의 취약점을 부각시킨 후, 이를 구조적으로 보완하며 컴퓨터의 속도에 의존하여 발전한 해독법이 아닌 현재 제시되어지고 있는 암호 해독방법에 의한 공격에서도 내성을 지니도록 보완된 알고리즘을 제안한다. 이 방식을 통해 보완된 관제신호 보호 알고리즘은 입력으로 사용되는 원격명령신호 데이터의 크기와 메시지 인증 코드의 크기를 변경하지 않아 기존의 위성 시스템에 그대로 적용 가능하다는 장점을 지닌다.

Ⅱ. 위성 암호 시스템

지상 관제 국으로부터 위성으로 전송하는 명령신호가 정당한 지상 관제 국에서 보내온 신호인지를 확인하고 명령신호의 무결성을 확인하는 관제신호 보호 알고리즘으로 블록 암호 알고리즘을 이용한 메시지 인증 코드(Message Authentication Code, MAC)를 사용한다[4].

1. 메시지 인증 코드

메시지 인증 코드는 다음과 같은 형태의 함수 C와 비밀키 K에 의해 생성되는 고정된 크기의 데이터 블록이다

$$MAC = C_K(x) \tag{1}$$

위 식에서 x는 가변 길이 메시지이고, K는 송신자와 수신자 사이에서만 공유된다고 가정되는 비밀키이다. 송신자는 전송할 메시지와 키를 사용하는 함수로서 메시지 인증 코드를 계산한 후 전송할 메시지에 부가하여 수신자에게 전송한다. 수신자는 수신된 메시지에 비밀키를 이용하여 새로운 메시지 인증 코드를 생성하여 수신된 메시지 인증 코드와 비교한다. 기본적인 사용법은 그림 1과 같다.

이때 송신자만이 비밀키를 알고 있다고 가정하였으므로, 수신된 메시지 인증 코드와 계산된 메시지 인증 코드 값이 일치한다면 수신자는 메시지가 변경되지 않았다고 확신한다. 공격자는 비밀키를 모른다고 가정되기 때문에 공격자는 메시지의 변경과

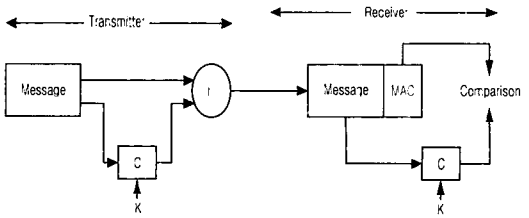

그림 1. 메시지 인증 코드의 기본 사용그림

일치하게 메시지 인증 코드를 수정할 수 없다. 공격자가 메시지를 변경하고 메시지 인증 코드를 변경하지 않았다면 수신자의 메시지 인증 코드 계산 값은 수신된 메시지 인증 코드와 다를 것이다. 그러므로 수신자는 메시지가 공격자에 의하여 위조 혹은 변조되었음을 알고 메시지를 인증하지 않음으로 메시지의 무결성을 확인할 수 있다. 또한, 수신자는 메시지 인증 코드로 인하여 정당한 송신자로부터 메시지가 왔음을 확신할 수 있다. 공격자는 비밀키를 모르기 때문에 적절한 메시지 인증 코드를 생성해 메시지를 준비할 수 없기 때문이다. 이와 같이 메시지 인증 코드 알고리즘은 데이터의 무결성(integrity)과 데이터 생성, 인증뿐만 아니라 사용자 식별(identification)의 기능도 제공한다.

2. CBC-MAC

블록 암호 알고리즘을 기반으로 하는 메시지 인증 코드 알고리즘들 중에서, DES를 CBC(Cipher Block Chaining)모드로 운용하는 CBC-MAC은 가장 널리 사용되어지고 있다. 이 방식은 금융권에서 무결성의 목적으로 ANSI표준(X9.17)과 ISO/IEC 9797으로 표준화되어 사용되고 있으며, 저렴한 구현 비용으로 인하여 디지털 서명 및 스마트카드, IP (Internet Protocol) 레벨의 보안을 유지하기 위하여 널리 사용되고 있다. 알고리즘의 블록 암호는 DES를 사용하므로 입력 메시지의 길이 n은 64 비트이고 키 K는 56 비트가 된다. CBC-MAC는 암호화할 때 바로 앞 블록의 암호문 출력과 입력 블록을 XOR(exclusive-OR)하는 방법을 사용하며 동작과정은 아래와 같다[6]-[7].

단계1 : 입력 메시지 x에 필요한 경우 패딩을 하여 64 비트의 크기로 나누어서 블록 x_1, x_2, ... , x_t로 구분한다.

단계2 : CBC 모드의 블록 암호를 키 K를 이용하여 아래와 같이 동작시켜 H_t를 얻는다.

$$H_1 = e_K(x_1) \quad (2)$$

$$H_i = e_K(x_i \oplus H_{i-1}) \text{ for } i = 2, 3, ..., t \quad (3)$$

단계3 : H_t에서 상위 m비트를 절단(truncate)하여 최종 MAC을 형성한다.

CBC-MAC은 DES의 안정성에 기반을 두고 있으며 그 안정성에 대한 평가가 이미 이루어져 있다[6]. 블록 암호 DES를 기반으로 하는 CBC-MAC은 블록 알고리즘이 하드웨어 실행에 적합하게 설계가 되어 있어, 소프트웨어 실행 시에 지약을 받는 단점이 있다. 그래서 최근에는 소프트웨어 실행에 적합하게 설계된 해쉬 함수를 기반으로 하는 많은 메시지 인증 방식에 대한 연구가 추진되고 있으나 DES를 기반으로 하는 메시지 인증 방식보다 속도 면에서는 우수하나 인증 방식의 안정성이 증명이 되지 않는 단점이 있어[4] CBC-MAC이 널리 사용되고 있으며 관제신호 보호 알고리즘으로도 이 방식이 응용되어 사용된다.

3. 관제신호 보호 알고리즘

위성통신의 관제신호 채널에서 지상 관제소로부터 위성체로의 원격명령신호 전송에 사용되어 보안 서브시스템을 이루어 메시지 인증 코드를 계산하기 위하여 소프트웨어를 탑재한다. 지상의 컴퓨터는 위성으로 원격명령신호를 송신하기 전에 이 소프트웨어를 구동하여 적절한 메시지 인증 코드를 원격명령신호에 추가한 후 송신한다. 소프트웨어에 사용되는 알고리즘은 위에서 언급한 CBC-MAC의 형태에 기반을 두고, 입력 메시지 블록을 2단으로 제한하며 블록 암호로는 DES를 사용한다.

x_1과 x_2는 각 64 비트의 입력 메시지이며 필요할 경우 '0'을 패딩한다. 입력 메시지는 위성으로 전송하는 원격명령신호의 일부분과 위성에서 내려 받은 순간적인 값을 함께 사용한다. 위성체에서 내려 받은 값은 위성체내의 상태에 따라서 시간적으로 계속해서 바뀌는 값이며 위성체는 이 값을 원격측정 신호를 통하여 지상 관제소로 전달한다.

이렇게 만들어진 입력 메시지는 지상 관제소와 위성체만이 가지는 64 비트의 비밀키 K를 이용하여

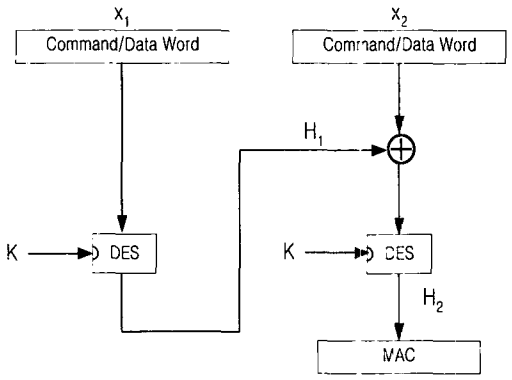

그림 2. 관제신호 보호 알고리즘의 동작과정

CBC-MAC의 형태로 암호화되고 그 출력 값을 메시지 인증 코드로 원격명령신호에 덧붙여서 위성으로 전송한다.

위성체에서는 메시지를 수신하면 메시지 인증 코드를 제외한 원격명령신호와 지상으로 전송한 위성체 내의 정보를 지상에서와 동일한 알고리즘으로 수행하여 메시지 인증 코드를 계산하고 수신된 메시지 인증 코드와 비교한다. 계산된 메시지 인증 코드와 수신된 메시지 인증 코드가 같게 되면 정당한 지상 관제소에서 보내온 원격명령신호임을 확인하고 인증하게 된다. 그러면 위성은 원격명령신호에 따라 위성체내의 설정이나 각 부분의 역할 변화 등의 주어진 임무를 수행하게 된다. 만일 메시지 인증 코드가 같지 않으면 인가되지 않은 사용자의 개입으로 간주하고 임무를 수행하지 않는다.

4. 관제신호 보호 알고리즘의 취약점 도출

위성 암호는 위에서 살펴본 바와 같이 CBC-MAC을 기반으로 하고 있다. CBC-MAC에서의 알려진 공격방법은 키 복구 공격(key recovery attack)과 위장공격(forgery attack)이 있다[7]. 키 복구 공격은 위장공격보다 더욱 강력한 공격이라고 할 수 있다. 공격자가 비밀키를 복구할 수 있다면 모든 메시지에 대한 위장공격이 가능하다.

키 값을 정확하게 구해내는 키 복구 공격 중에서는 가능한 키 값을 바꾸어 가며 모두 수행하여 키 값을 찾아내는 전수공격(exhaustive search)이 가장 일반적으로 사용되어지고[8], 최근에는 평문에 대응하는 암호문 쌍들을 이용하여 키를 복구하기 위한 연산의 횟수를 줄이는 기지 평문 공격(known-plain text attack)도 활발히 연구되고 있다.

두 번째 공격 방법인 위장 공격은, 정확한 비밀키를 구하지 않으면서 특정한 메시지에 유효하지 않은 메시지 인증 코드 값을 덧붙여 제출하더라도 인증 시스템을 통과하여 공격할 수 있는 방법이다[9]~[10]. 이 방법은 생일 역설에 의해서 입력은 다르지만 출력 값이 같은 충돌쌍이 하나 이상 존재하는 기지 평문-암호문 쌍을 알 경우를 배경으로 한다. 이 경우 충돌 암호문에 임의의 메시지를 연접하여, 비밀키를 알지 못한 경우에도 선택 평문에 대해 정당한 메시지 인증 코드값을 생성할 수 있다. 그러나 이 위장 공격은 길이가 다른 메시지에 의한 위장은 쉽게 가능하나, 관제신호 보호 알고리즘과 같이 동일한 길이의 메시지를 입력으로 사용하는 경우에는 비교적 안전하다.

관제신호 보호 알고리즘의 안정성에 대한 평가를 내리기 전에 안정성의 기준을 살펴보아야 한다. 98년 Rivest는 계산상 불가능(computationally infeasible)의 기준을 2^{64} 이상의 계산 복잡도가 요구되는 것으로 설정하였고[11], 최근에는 컴퓨터의 연산속도의 증가와 병렬처리 기술의 발달로 인해 2^{80} 이상의 계산 복잡도를 계산상 불가능으로 설정하는 것이 바람직하다고 권고한다[5].

이를 기준으로 하여 관제신호 보호 알고리즘의 안정성에 대하여 살펴보면, 현재의 관제신호 보호 알고리즘은 메시지 길이를 2 단으로 제한하므로 위장공격에는 어느 정도 안전하다고 볼 수 있지만, 2단에 걸쳐 DES 알고리즘을 두 번 사용하면서도 실제로는 56 비트의 비밀키 K만을 사용하므로 하나의 기지 평문-암호문쌍만 주어진다면 DES의 짧은 키 길이로 인해 기본적 공격인 전수공격에 의해서 2^{55} 번의 시도로 정확한 키 값이 복구되므로 충분한 안정성을 가지지 못한다. 이 값은 Rivest의 권고안인 2^{64} 에도 미치지 못하는 값이므로 관제신호 보호 알고리즘의 개선이 반드시 필요함을 알 수 있다.

Ⅲ. 개선된 관제신호 보호 알고리즘의 제안

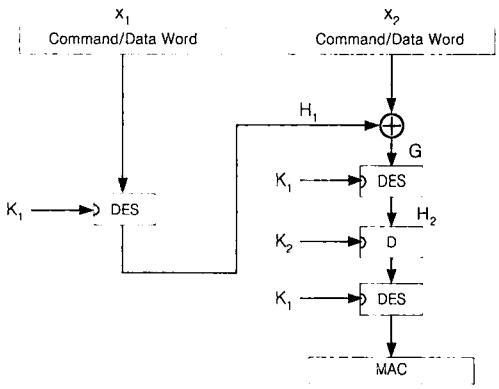

그림 3. Retail MAC을 이용한 관제신호 보호 알고리즘

1. Retail MAC을 적용한 개선

CBC-MAC의 안정성을 증가시키기 위한 방법으로는 출력 변환(output transformation)을 마지막 블록에 덧붙이는 방법을 가장 일반적으로 사용하고 있다. 즉, 단계 t에서 얻어진 H_t에 출력 변환 g를 부가적으로 처리하여 $MAC_K(x) = g(H_t)$를 생성한다. 단계 t의 결과인 H_t를 두 번째 키 K_2를 사용하여 복호화하고 다시 K_1을 사용하여 암호화하는 트리플 DES의 형태를 출력단에 적용한 방법이 가장 보편

적으로 사용되며 이 방법은 강화된 CBC-MAC으로써 ANSI 표준(retail MAC)에 채택이 되어 사용되고 있다[12]. 이 방식을 관제신호 보호 알고리즘에 적용하면, 두 번째 키 K_2의 사용으로 키 길이를 늘일 수 있다. 관제신호 보호 알고리즘으로 retail MAC을 적용한 구조는 그림 3과 같다.

관제 신호 보호 알고리즘에도 동일한 기능을 가지는 블록을 덧붙여서 나타내었다. 여기에서 D는 복호화를 의미하며 새로운 키 K_2가 사용이 되었으므로 키 길이가 56 비트에서 112 비트로 늘어나게 된다. 키 값이 늘어났으므로 새로운 키 관리에 대한 방안이 더 필요하게 되었지만 기존 시스템의 큰 변화 없이 알고리즘의 보완 방법을 제시하였다.

위와 같은 출력 변환을 덧붙인 후의 안정성에 대하여 검토 해보자. 키 길이가 112 비트로 늘어나게 되어 전수공격으로 정확한 비밀키 K_1과 K_2를 찾아내기 위해서는 2^{111} 번의 수행이 필요하게 된다. 단지 위와 같이 전수공격만을 고려한다면 retail MAC을 적용한 이 알고리즘은 Rivest의 권고안뿐만이 아니라 최근에 요구되어지고 있는 2^{80} 라는 복잡도 권고안을 충분히 만족하게 된다. 그러나 retail MAC을 이용한 알고리즘은 고정된 2 단만을 이용한다는 관제신호 보호 알고리즘 특성에 의해 Preneel이 제안한 공격법[12]의 적용 시 전수공격을 적용한 경우와 비교하여 키 복구를 위한 시행횟수를 현격히 줄일 수 있다.

2. Retail MAC을 적용한 개선방안의 취약점

CBC-MAC에서 키 길이의 증가를 위해 출력단에 트리플 DES의 형태를 도입한 retail MAC은 Preneel이 제안한 공격에 의하면 충돌이 일어나는 $2^{(n+1)/2}$ 개의 기지 평문쌍과 $(2t-1)\times 2^k$ 번의 암호화 수행만으로 정확하게 키 K_1과 K_2가 복구되어 질 수 있다[9]. 여기에서 n은 입력평문의 길이이며 t는 입력 메세지 단의 개수이다. Retail MAC을 이용한 알고리즘에 Preneel의 공격을 적용하면 다음과 같다.

단계1 : 생일 역설에 의해서 64비트의 출력에 대하여 한 개 이상의 충돌 쌍이 생기는 최소의 기지 평문-암호문쌍의 개수는 $2^{32.5}$ 이므로, $2^{32.5}$ 의 기지 평문쌍에서 입력값이 다른 메시지에 대하여 같은 메시지 인증 코드값이 생성되게 되는 충돌쌍 (X,Y)와(X*,Y)를 찾는다. 이 경우에 출력 변환은 K_1과 K_2를 이용한 동일 연산을 수행하므로 G 에서의 값 역시 충돌을 일으키게 된다.

단계2 : x_1을 2^{56} 개의 키 값으로 암호화하여 모든 H_1을 구해내고 그 값을 x_2와 XOR하여 모든 G를 구한다.

단계3 : x^*_1을 2^{56} 개의 키 값으로 암호화하여 모든 H^*_1을 구해내고 그 값을 x^*_2와 XOR하여 모든 G*를 구한다.

단계4 : G = G*의 충돌을 발생하지 않는 키들을 제거한다. 키의 길이 56 비트는 블록 데이터의 길이 64 비트보다 작으므로 유일한 키를 결정할 수 있으며, 유일한 키는 K_1이 된다.

단계5 : 단계 4의 K_1과 충돌값 G를 이용하여 아래의 식을 구한다.

$$G' = E_{K1}(G) \quad (4)$$

$$G'' = D_{K1}(MAC(x)) \quad (5)$$

단계6 : G'와 G'' 에 대하여 K_2를 찾기 위한 전수공격을 하여 2^{56} 번의 시도로 $D_{K2}(G') = G''$를 만족하는 K_2를 찾는다. 이때 키 길이가 블록 데이터 길이보다 작으므로 한 번의 전수공격으로 K_2를 찾을 수 있다.

결과를 정리하면 충돌 쌍을 찾아내기 위한 기지 평문-암호문쌍 $2^{32.5}$ 개가 필요하며 2 단계와 3 단계에서의 각 2^{56} 번과 마지막 6 단계 전수공격에서의 2^{56} 번의 암호화 수행이 필요하므로 전체 3×2^{56} 번의 암호화 수행이 필요하다. 전수공격에 대해서는 2^{111} 번의 수행이 필요하여 권고안을 만족했지만 Preneel이 제안한 공격에 의해서는 기지 평문-암호문쌍 $2^{32.5}$ 개와 3×2^{56} 의 수행만으로 키 복구가 이루어져 Rivest의 권고안과 최근에 요구되어지는 2^{80} 의 권고안을 만족하지 못한다. 즉, 오직 2 단만을 이용하는 관제신호 보호 알고리즘의 특징으로 인해 일반적인 CBC-MAC을 보완하는 방법으로는 충분한 안전성을 제공하지 않는다. 따라서 관제신호 보안 방법 개선의 필요성은 여전히 존재하게 된다.

3. 새로운 관제신호 보호 알고리즘의 제안

출력 변환을 이용하여 출력 단을 트리플 DES 형태로 변형하는 retail MAC을 이용한 관제신호 보호 알고리즘은 짧은 단의 길이로 인하여 Preneel의 공격에 대해 충분한 안정성을 가지지 못하였다. Preneel의 공격은 출력 변환을 무시하고 충돌이 발생한 기지 평문 쌍으로부터 ($H_{t-1} \oplus x_t$) 즉, 동일한

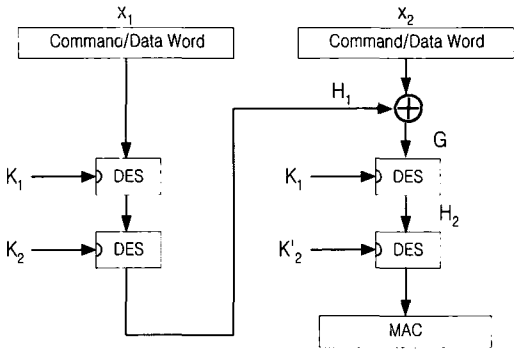

그림 4. 제안된 관제신호 보호 암호 알고리즘

G = G* 를 생성하는 키에 전수공격을 함으로써 연산 횟수를 줄인다. 그러므로 이 Preneel의 공격에 대한 보완은 G를 찾기 위한 공격이 Rivest의 권고안을 만족하도록 키의 크기를 증가시키므로 이루어질 수 있다. 즉, 두 번째 키 K_2를 출력 변환에서만 이 아니라 초기변환으로도 이용하는 방법이다. 새로운 키를 초기변환과 출력변환에 적용하는 대표적인 방법은 MacDES 알고리즘이다[13]. 그러므로 우리는 MacDES 알고리즘을 적용하여 현재 관제신호 보호 알고리즘의 초기변환과 출력변환을 단일 DES에서 더블 DES로 바꾸어주는 새로운 관제신호 알고리즘을 제안한다. 이 방법을 적용시킨 관제신호 보호 알고리즘의 알고리즘은 아래와 같다.

새로운 알고리즘을 적용하여 메시지 인증 코드를 생성하는 과정은 다음 식 (6)~(8)으로 표현된다.

$$H_1 = E_{K2}(E_{K1}(x_1)) \quad (6)$$

$$H_2 = E_{K1}(H_1 \oplus x_2) \quad (7)$$

$$MAC_K(x) = E_{K'2}(H_2) \quad (8)$$

여기에서 K'_2는 K_2와는 다른 값으로 $K'_2 = K_2 \oplus \beta$ 로 정의되어지며 이때 는 '0'이 아닌 56 비트 열이 된다. 더블 DES를 입력과 출력에 적용하여 K_1에 의한 암호화와 K_2를 이용한 암호화가 연달아 수행되므로 기지 평문-암호문 쌍에 의한 키 복구 공격에 강한 안정성을 가지게 되고 중간공격에 의한 공격을 피하기 위하여 출력 단에서는 K_2 대신에 K'_2를 사용하였다. 또한 키 길이가 112 비트로 늘어남으로 전수공격에 의한 안정성도 기본적으로 증가하여 2^{111} 번의 수행이 필요하므로 이 값은 Rivest 권고안과 최근 요구되고 있는 계산 복잡도를 충분히 만족시킨다.

제안한 방법은 retail MAC에 의한 개선과 마찬가지로 키 길이가 112 비트가 되므로 별도의 키 K_2의 관리가 필요하고 사용된 DES의 수가 4번으로 동일하므로 같은 계산량을 가진다. 따라서 전수공격에 의한 안정성과 메시지 인증 코드를 생성하는데 걸리는 시간도 동일하다. 그러나 retail MAC은 최근 연구에 의한 기지 평문-암호문 쌍을 이용한 키 복구 공격에서는 취약하여 복잡도 권고안을 만족시키지 못하였으나 제안한 방법은 안정성이 크게 증가하여 권고안을 모두 만족시킨다. 관제신호 보호 알고리즘이 위성을 제어하는 원격명령신호의 전달 채널을 보호하기 위한 알고리즘이므로 알고리즘의 수행시간은 위성의 실시간 제어와 매우 관련성이 높다. 알고리즘의 안정성이 매우 커진다 하더라도 수행시간이 매우 길어진다면 위성제어의 실시간 처리 특성에 제약을 주게 되므로 좋은 개선 방안이 되지 못한다. 제안한 방법과 같이 기존의 방법에 의한 개선 알고리즘과 수행시간이 동일하면서 안정성의 증가가 크게 이루어진다면 매우 효율적으로 관제신호 보호 알고리즘이 개선된다고 할 수 있다.

Ⅳ. 실험 및 고찰

제안한 관제신호 보호 알고리즘의 안정성을 검증하기 위해 컴퓨터 시뮬레이션으로 retail MAC을 적

표 1. 관제신호 보호 알고리즘 수행시간과 키 복구 시간

	관제신호 보호 알고리즘 (기존사용 방법)	관제신호 보호 알고리즘 (Retail MAC 적용)	관제신호 보호 알고리즘 (제안한 방법)
수행시간	377 μsec	762 μsec	759 μsec
14 비트 키 복구	3 sec	6 sec	6 sec
21 비트 키 복구	395 sec	799 sec	795 sec
56 비트 키 복구	1.36×10^{13} sec	2.75×10^{13} sec	2.77×10^{13} sec
112 비트 키 복구		1.98×10^{30} sec	2.00×10^{30} sec

용한 개선방법과 비교하여 수행시간과 전수공격에 대한 안정성이 동일함을 확인하고, Preneel의 공격법을 제안한 관제신호 보호 알고리즘에 적용하여 키 복구 공격에 대한 안정성이 증가하였음을 확인한다.

1. 컴퓨터 시뮬레이션

제안한 알고리즘이 키 길이의 증가로 인하여 현재 사용되고 있는 관제신호 보호 알고리즘에 비하여 전수공격에 대해 안정성이 크게 증가하고, 일반적인 CBC-MAC 개선방법인 retail MAC의 적용과 수행속도를 비교하기 위하여 컴퓨터 시뮬레이션을 수행하였다. Pentium Ⅲ 866MHz의 PC에서 C언어를 사용하여 구현하였다. 우선 알고리즘을 한번 수행하는데 걸리는 시간인 수행시간을 구하고, 이어서 가능한 모든 키를 적용하여 정확한 키를 찾는 전수공격에 걸리는 시간을 측정하였다. 키 공간은 소프트웨어적으로 시뮬레이션을 가능토록 하기 위하여 실제 키 공간 중 14 비트와 21 비트만을 사용하고 한 쌍의 입력과 출력 메시지 인증 코드 값을 주어 실험하였다. 시간상의 제약으로 56 비트와 112 비트에서의 실험은 실제적으로 수행한 값이 아니라 14 비트와 21 비트의 실험을 바탕으로 계산상으로 구한 값이다.

수치적으로도 계산 복잡도 권고안을 만족함을 확인한 바 있으며, 실험 결과로부터 제안한 방법은 전수공격에 의한 키 복구 시간이 기존의 방법보다 두 배 정도가 소요되어 안정성이 증가함을 확인할 수 있다. 또한 기존의 보완방법인 retail MAC을 적용한 관제신호 보호 알고리즘과 수행속도 면에서 시간상의 차이가 없음을 알 수 있다.

2. Preneel 공격의 적용

Retail MAC을 적용하여 관제신호 보호 알고리즘을 개선시킨 방법과 제안한 방법은 컴퓨터의 계산속도에 의존하는 전수공격에 대한 안전성 면에서 동일하다. 그러나 암호 해독기술의 발전에 따른 키 복구 공격에는 취약하여 개선점이 여전히 남아 있음을 앞에서 확인하였다. Preneel의 공격법을 제안한 알고리즘에 적용하여 retail MAC에 의한 보완보다 제안한 방법이 안정성이 더욱 우수하며 수치적으로 최근까지의 권고안을 모두 만족시킨다는 것을 검증한다.

기존 방법인 retail MAC에 의한 개선 알고리즘의 공격과 마찬가지로 Preneel의 공격을 적용하면 아래와 같다.

단계1 : 앞에서와 마찬가지로 $2^{32.5}$ 의 기지 평문-암호문쌍에서 다른 메시지에 대하여 같은 메시지 인증 코드값이 생성되게 되는 충돌쌍 (X,Y)와 (X*,Y)를 찾는다. 이 경우에 G 이하의 부분은 동일한 연산을 수행하는 부분이 되므로 G에서의 값도 충돌을 일으키게 된다.

단계2 : x_1에서 K_1과 K_2에 해당하는 2^{112} 개의 키 값으로 암호화하여 H1을 구해내고 그 값을 x_2와 XOR한다. 이 값을 G라 한다.

단계3 : x*1에서 K_1과 K_2에 해당하는 2^{112} 개의 암호화하여 H^*_1을 구해내고 그 값을 x_2와 XOR한다. 이 값을 G*라 한다.

단계4 : G = G*의 충돌을 발생하지 않는 키들을 제거한다. 키의 길이 112 비트는 블록 데이터의 길이 64 비트보다 크므로 주어진 평문 x_1에 대해여 G = G*의 조건을 만족하는 키의 수는 평균적으로 $2^{112}/2^{64} = 2^{48}$ 개이며, 유일한 K_1과 K_2를 결정하기 위해서는 다른 충돌쌍이 필요하게 된다.

단계5 : 기지 평문-암호문쌍의 수를 늘려 다른 충돌쌍을 찾아 단계 2, 3, 4를 다시 수행한다. 이 과정으로 유일한 K_1과 K_2를 결정할 수 있다.

결론적으로 단계 2와 단계 3에서 각각 2^{112} 번의 암호화 과정이 필요하고 키 길이가 메시지 인증 코드의 길이보다 길어 이 과정이 두 번 수행되어야 하므로 $2\times2\times2^{112} = 2^{114}$ 번의 수행이 필요하고 두 개의 충돌 쌍을 찾기 위해 $2^{32.5}$ 이상의 기지 평문-암호문쌍이 필요하다. 따라서 2^{114} 의 계산 복잡도는 위에서 언급한 Rivest 권고안과 최근에 요구되어지는 계산 복잡도 권고안 2^{80} 을 충분히 만족하므로 제안한 관제신호 보호 알고리즘은 전수공격만이 아니라 Preneel의 공격에 대해서도 충분한 안정성을 제공한다.

살펴본 바와 같이 제안한 방법은 retail MAC에 의한 개선과 같은 수행시간을 가지면서 Preneel 방법에 의한 키 복구 공격에는 안정성의 증가가 크게 이루어짐을 알 수 있다. 또한 안정성을 증가시키면서도 입력 메시지의 길이와 출력 메시지 인증 코드의 길이는 기존의 알고리즘과 동일하게 유지할 수 있게 된다. 이로 인하여 위성 체와 지상 관제소가 주고받는 패킷의 구조와 길이를 동일하게 사용할 수 있으므로 현재의 위성관제 시스템의 변경 없이 더욱 안전하게 관제신호를 보호할 수 있다는 장점

을 가지게 된다.

V. 결 론

본 논문에서는 위성의 위치, 성능, 그리고 동작을 제어하는 관제신호의 보호를 위하여 사용되는 관제 신호 보호 알고리즘의 취약점을 도출하고 이를 개선하기 위한 새로운 알고리즘을 제안한다. 우선 현재 사용되고 있는 관제신호 보호 알고리즘의 취약점을 개선하기 위해 키 길이의 증가가 필요함을 기술하고, CBC-MAC의 일반적인 개선방법인 retail MAC을 적용함으로써 새로운 키를 도입하여 키 길이를 증가시켰다. 그러나 기지 평문-암호문 쌍을 이용한 키 복구 공격에는 여전히 충분한 안전성을 가지지 못하므로, 본 논문에서는 관제신호 보호 알고리즘의 초기변환과 출력변환에서 새로운 키를 도입하는 방법을 사용하여 안정성을 확보한다. 제안한 알고리즘의 안정성을 검증하기 위하여 컴퓨터 시뮬레이션을 통한 시간 측정과 Preneel의 공격을 사용하였다.

제안한 알고리즘은 retail MAC을 적용한 개선방법과 같은 복잡도를 가지므로, 수행시간이 동일하면서도 기지 평문-암호문 쌍을 이용한 키 복구 공격에 강하게 설계되어 현재 권고되고 있는 계산 복잡도를 만족하여 충분한 안전성을 가진다. 위성의 실시간 제어를 고려한다면 retail MAC에 의한 개선과 비교하여 수행시간의 증가 없이 안정성이 확보되므로 매우 효율적인 개선방법이라고 볼 수 있다. 또한 입력으로 사용되는 관제신호 데이터의 크기와 메시지 인증 코드의 크기를 변경하지 않아 기존의 위성 시스템에 그대로 적용 가능하며 키 복구 공격에 대한 계산 복잡도를 기존의 2^{55} 번의 수행에서 2^{111} 번으로 증가시켜 Rivest의 권고안을 만족시킨다.

참 고 문 헌

[1] 이호진, "위성관제 기술," 전자공학회지, 제 19권, 제 10호, pp. 968-981, Dec. 1992

[2] 김영신, 김천휘, 김경희, 방효충, "무궁화 위성의 원격측정 자료 처리기법," 한국우주과학회지, 제 13권, 제 2호, pp. 235-245, May 1996

[3] 김명석, "무궁화 위성 지상관제 시스템과 운용소프트웨어," 한국통신학회, 제 12권 제 6호, Jun. 1996

[4] 홍기웅, 최완식, 이호진, 김동규, "메세지 인증 코드 기법을 이용한 위성명령 보안 메커니즘," 한국통신정보보호학회 종합학술발표회논문집, pp. 99-107, Nov. 1994

[5] 강주성, 김재헌, 박상우, 박춘식, "현대암호학," ETRI 부설 국가보안기술연구소, 경문사

[6] A.J. Menezes, P.C. van Oorshot, S. Vanstone, "Handbook of Applied Cryptography," CRC Press, Boca Raton, 1997

[7] Mihir Bellare, Joe Killian, Phillip Rogaway, "The Security of the Cipher Block Chaining Message Authentication Code," Journal of Computer and System Sciences, Vol. 61, No. 3, pp. 362-399, Dec. 2000

[8] Mihir Bellare, R. Canetti, H. Krawczyk, "Keying hash functions for message authentication," Advances in Cryptology-CRYPTO'96, Springer-Verlag, Lecture Notes in Computer Science, Vol. 1109, pp. 1-15, Jun. 1996

[9] K. Brincat and C.J. Mitchell, "New CBC-MAC forgery attacks," Information Security ,and Privacy, Springer-Verlag, Lecture Notes in Computer Science, Vol. 2119, pp. 3-14, Jul. 2001

[10] L.R. Knudsen, "Chosen-text attack on CBC-MAC," Electronic Letters, Vol. 33, No.1, pp. 48, Jan. 1997

[11] R.L. Rivest, "The MD4 Message Digest Algorithm," Crypto'90, Springer-Verlag, Lecture Notes in Computer Science, Vol. 537, pp. 303-311, Apr. 1991

[12] B. Preneel, P.C. van Oorschot, "Key recovery attack on ANSI X9.19 retail MAC," ,Electronic Letters, Vol. 32, No. 17, pp. 1568-1569, Aug. 1996

[13] Knudsen, B. Preneel, "MacDES:MAC Algorithm based on DES," Electronic Letters, Vol. 34, No. 9, pp. 871-873, Apr. 1998

곽 원 숙(Won-sook Kwak) 준회원

2001년 2월 : 경북대학교 전자공학과 졸업
2001년 3월~현재 : 경북대학교 전자공학과 석사과정
<주관심 분야> 위성통신, 무선통신, 정보 보호

조 정 훈(Jeong-hoon Cho) 준회원

1998년 2월 : 경북대학교 전자공학과 졸업
2000년 2월 : 경북대학교 전자공학과 석사
2000년 3월~현재 : 경북대학교 전자공학과 박사과정
<주관심 분야> 위성통신, 무선통신, 정보 보호, 인증 알고리즘

홍 진 근(Jin-keun Hong) 정회원
1991년 2월 : 경북대학교 전자공학과 졸업
1994년 2월 : 경북대학교 전자공학과 석사
2000년 2월 : 경북대학교 전자공학과 박사
1998년 2월~2001년 8월 : 창신대학 정보통신과 조교수
2001년 9월~현재 : 국가보안기술 연구소 연구원

박 종 욱(Jong-wook Park) 정회원
1986년 2월 : 경북대학교 전자공학과 졸업
1988년 2월 : 경북대학교 전자공학과 석사
2001년 2월 : 경북대학교 전자공학과 박사
1998년~2000년 : 국방과학연구소
2001년~현재 : 국가보안 기술 연구소 연구원

김 성 조(Sung-jo Kim) 정회원
1983년 2월 : 경북대학교 전자공학과 졸업
1985년 2월 : 경북대학교 전자공학과 석사
1985년~2001년 : 한국전자통신연구원
2001년~현재 : 국가보안기술연구소 연구원
<주관심 분야> 위성통신기술, 정보보호기술

윤 장 홍(Jang-hong Yun) 정회원
1982년 2월 : 경북대학교 전자공학과 졸업
1987년 2월 : 경북대학교 전자공학과 석사
1997년 2월 : 경북대학교 전자공학과 박사
1983년~2000년 : 국방과학연구소 개발팀장
2000년~현재 : 국가보안기술연구소 개발팀장

이 상 학(Sang-hak Lee) 정회원

1984년 2월 : 경북대학교 전자공학과 졸업
1986년 2월 : 경북대학교 전자공학과 석사
2001년 8월 : 경북대학교 전자공학과 박사
2000년 3월~현재 : 동양대학교 정보통신공학부 전임강사
<주관심 분야> 데이터통신, 영상신호처리

황 찬 식(Chan-sik Hwang) 정회원

1977년 2월 : 서강대학교 전자공학과 졸업
1978년 2월 : 한국과학기술원 석사
1996년 2월 : 한국과학기술원 공학박사
1980년 3월~현재 : 경북대학교 전자공학과 교수
<주관심 분야> 데이터 통신, 영상신호처리, 암호통신