CBC-MAC 방식을 적용한 보안 모바일기기 제어시스템

황재영* · 최동욱* · 정연호**

Secure Mobile-in-Vehicle System with CBC-MAC authentication

Jae-young Hwang* · Dong wook Choi* · Yeon-ho Chung**

본 논문은 교육과학기술부의 재원으로 한국연구재단의 지원을 받아 수행된 2009년도 광역경제권 선도사업 인재양성사업의 연구 결과입니다

요 약

모바일 기기 기반의 제어시스템에서 정보 해킹과 유출에 대비한 보안기능의 적용이 요구되고 있다. 이를 위한 보안 기술로서 가장 일반적인 방법은 암호와 인증이다. 본 연구에서는 보안 기능이 취약한 모바일 기기 기반의 제어 시스템에 있어서 효율적인 인증 방식 중 하나인 CBC-MAC (Cipher Block Chaining-Message Authentication Code)을 사용하여 외부의 공격으로부터 정보를 보호하는 CBC-MAC 기반의 보안 모바일기기 제어시스템 (SMIV: Secure Mobile in Vehicle)을 제안한다. CBC-MAC 은 송신측과 수신측에 비밀 키를 공유함으로써 전송된 정보가 변경되지 않고 본래의 정보임을 보증하는 방식이다. 제안 시스템의 검증을 위하여 모바일 기기 제어 시스템의 H/W 및 S/W를 구현하고 CBC-MAC 인증 방식을 적용하였다. 기존 연구에서는 모바일 기기를 이용한 제어시스템에서 보안성보다는 개선된 제어 방식이 주로 보고되고 있다. 본 연구에서는 모바일 기기를 이용한 제어시스템에서 보안성을 제고한 모바일 기기 제어시스템을 제안하며 이러한 보안 제어 시스템은 향후 모바일 기기를 이용한 각종 제어 시스템 설계 및 구축에 유용하게 사용될 것이다.

ABSTRACT

Demand on information security in mobile devices based control system grows rapidly with a view to counteracting information hacking and leakage. Among these techniques, encryption and authentication are most common. This paper presents CBC-MAC (Cipher Block Chaining-Message Authentication Code) based mobile devices control system. The system is termed as Secure Mobile in Vehicle (SMIV)We use CBC-MAC that is one of the most efficient authentication modes to protect information against any malicious attacks. By sharing the secret key of CBC-MAC between the transmitter and receiver, it asserts authentic information. The proposed system is verified in such a way that we develop mobile devices control system, apply the CBC-MAC algorithm to the control system and validate the received data. Unlike conventional systems where the development of control mechanism in mobile devices based control systems is main concern, this proposed system offers a secure communication link of the data in mobile devices control system and therefore would be useful to the design and implementation of various mobile devices based control systems.

키워드

CBC-MAC, 인증, 모바일기기, 제어시스템, 보안

Key word

CBC-MAC, authenctication, mobile devices, control system, security

* 부경대학교 정보통신공학과
** 부경대학교 정보통신공학과 (교신저자, yhchung@pknu.ac.kr)

접수일자 : 2010. 06. 12
심사완료일자 : 2010. 08. 12

Ⅰ. 서 론

스마트폰의 하드웨어 및 소프트웨어의 기술 발전으로 다양한 응용 프로그램들이 등장하였고, 특히 다양한 장치들을 제어 할 수 있는 제어 시스템이 등장하여 스마트폰의 성장을 가져왔다. 그 중 Wi-Fi, WiBro, 3G 통신망을 이용하여 통신을 하는 프로그램에서 많은 보안상의 문제점이 발생하여 정보 보호 문제의 필요성이 대두되고 있다. 최근에는 국내외에 악성코드로 인한 피해가 발생하여 사회적인 이슈가 되고 있다 [1].

현재의 모바일기기를 통한 제어에서는 각종기기의 제어자체에만 치중하여 보안에 관한 면에서는 취약성을 가지고 있고 이로 인하여 많은 문제점을 잠재적으로 가지고 있다. 이에 본 연구에서는 모바일기기를 통하여 제어시스템을 구축하는 동시에 보안을 위한 인증 알고리즘 중 블록암호화 알고리즘인 CBC - MAC (Cipher Block Chaining - Message Authentication Code) 알고리즘 [2]을 적용하였다.

CBC-MAC 알고리즘은 블록암호기반 MAC 알고리즘으로서 하나의 키를 이용하여 보내는 메시지 일부를 암호화 하여 이를 메시지와 함께 송신하고 수신측에서는 암호화된 문장을 복호화를 통하여 수신된 메시지가 변경되지 않고 본래의 정보 그대로임을 확인하고 이를 보증하는 방식이다[3].

본 연구에서 제안하는 보안 모바일기기 제어 시스템의 검증을 위해 모바일 기기를 이용한 제어시스템 (MIV : Mobile In Vehicle)을 구축하였고, CBC-MAC 인증 알고리즘을 적용하여 정상적으로 메시지가 전송되고 복호화를 통하여 인증 과정이 정상적으로 이루어짐을 확인한다. 다시 말해, MIV 하드웨어 시스템을 실제 구현하여 제안하는 보안 알고리즘을 적용하여 시스템의 보안기능을 검증하였다. 여기서 실제 차량을 이용한 구현에는 제약이 따르므로 주행로봇을 이용하였으며 모바일 환경은 MS (Microsoft) 사의 윈도우 모바일 6.5 [4] 및 삼성전자의 옴니아Ⅱ 스마트폰 [5]을 사용하였다.

Ⅱ. CBC-MAC 인증 알고리즘

1. MAC (Message Authentication Code)

메시지 인증코드 (MAC)는 메시지에 대한 간섭을 막는 구조로 메시지가 변경되지 않고 본래의 메시지 그대로임을 보증하는 기능을 한다. 즉 수신자와 송신자만이 알고 있는 비밀 키를 이용하여 정상적으로 송수신이 이루어 졌음을 확인한다.

송신자는 메시지를 보낼 뿐만 아니라, MAC 함수에 의해서 계산된 MAC 값을 같이 보내게 되며, 수신자는 받은 메시지의 MAC값과 메시지와 비밀 키로 계산한 MAC값을 비교한다. MAC값이 불일치 하다면, 이 메시지는 인증에 실패한 것으로 간주하게 된다.

2. CBC-MAC

CBC-MAC은 블록 암호를 전술한 MAC 인증방법으로 바꾼 것으로 Key는 블록 암호화키로 사용하여 CBC 암호화 모드로 메시지를 암호화하고 일부를 (truncated) MAC 으로 사용한다.

CBC-MAC 방식에서 MAC를 구하는 방법은 식 (1)과 같다.

$$\begin{aligned} C_0 &:= IV \\ C_i &:= E\,(P_i \oplus C_{i-1}) \\ MAC &:= M \end{aligned} \tag{1}$$

식 (1) 에서 ⊕기호는 배타적 논리합을 나타내고 E()는 인코딩을 의미한다. C는 메시지를 암호화한 문자열로 i길이의 문자열을 가진다. C0은 첫 번째 암호화될 문자로 암호화할 때에는 이전의 암호 문자가 존재하지 않으므로, 초기 벡터 (IV: Initial Vector)라고 불리는 초기값이 사용된다. 본 연구에서는 초기벡터 (IV) 로 고전적인 정의에서 사용되는 '0'을 사용하였다.

C_i는 원문자열 P의 i번째 문자와 C_{i-1}, 즉 i-1 번째 암호화된 문자와 배타적 논리합의 연산을 먼저 구한뒤 인코딩하여 구한다. 여기서 인코딩 방법은 Vigenère 알고리즘 [6]을 사용하여 구한다. 그리고 M은 암호화한 문자열 C 중 k 번째 문자열 (truncated) 까지 구성되며 인증에 사용될 MAC 이 된다.

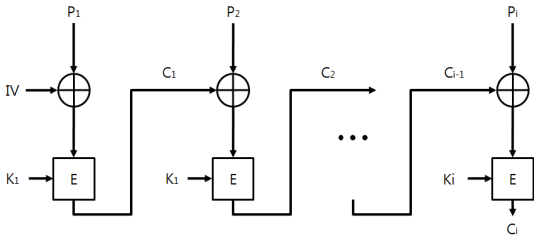


그림 1. CBC-MAC 블록 다이어그램
Fig.1 CBC-MAC block diagram

그림 1 은 전술한 CBC-MAC 구현 알고리즘을 블록 다이어그램으로 표현하였다. 그림에서 보면 원래 메시지와 키 값을 이용하여 암호화하고 이를 다음 문자의 암호화에 사용된다. CBC-MAC 은 그림1의 방법으로 암호화 한뒤 일부분 (k번째 문자열 까지)만 잘라내어 CBC-MAC 암호화 문자를 얻게 된다.

Ⅲ. 보안 모바일기기 제어 시스템

1. 모바일기기 제어시스템 구현

보안기능의 모바일 기기 제어시스템에 적용하기 전에 먼저 모바일기기 기반의 제어 시스템 (MIV) 을 구현하였다. MIV 시스템 구현은 사용자 인터페이스 및 차량 제어, 모바일 환경으로 나누어 구현하였다.

송신 측에서는 PC, PDA, 스마트폰을 이용하여 제어 메시지를 기지국 (Base station) 을 통하여 인터넷망에 접속한다. 그리고 수신측의 Base station을 통하여 수신측의 스마트폰에 접속하게 되어 메시지를 수신하며 이를 Micro controller를 통해 복호화 하여 주행로봇으로 제어 신호가 최종 전달된다.

여기서 본 연구에서 제안하는 보안 모바일기기 제어 시스템은 상기 제어 메시지에서 CBC-MAC 보안 알고리즘을 적용하여 인증 메세지를 생성한 뒤 전송하게 되며 수신측은 이를 복호하여 검증한 뒤 제어신호를 주행로봇으로 최종 전달하는 시스템이 된다.

그림 2 는 MIV 시스템의 개념도이다.

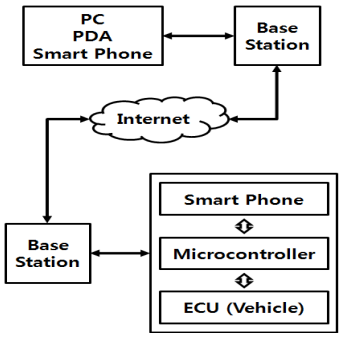


그림 2. MIV 시스템 개념도
Fig.2 Conceptual diagram of the MIV system

2. CBC-MAC 암호화 및 복호화 구현

2장에서 설명한 CBC 모드의 암호화 및 복호화 순서도는 그림 3과 같다.

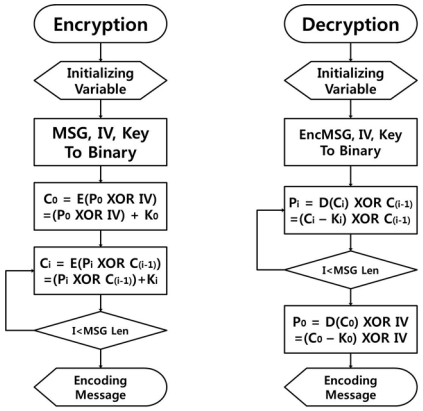


그림 3. CBC 암호화 및 복호화 순서도
Fig 3. Flowchart of encryption/decryption of CBC

위의 순서도에서 사용된 P, IV, K, C의 정의는 식 (2)와 같다.

$$P = \{P_0, \ldots, P_i\}$$
$$IV = \{IV\}$$
$$K = \{K_0, \ldots, K_i\}$$
$$C = \{C_0, \ldots, C_i\} \quad (2)$$

P는 암호화될 메시지이고 IV는 초기화 벡터이다. K는 송신자 및 수신자가 알고 있는 키 값이며, C 는 최종 암호화된 메시지이다. 이때 인코딩 및 디코딩은 Vigenère 암호 알고리즘을 사용하였다.

암호화 과정은 변수들을 초기화시키고 이를 이진수로 변환한다. 첫 번째 글자의 경우 메시지와 IV의 배타적 논리합을 계산한 후 이를 인코딩을 하여 구하게 된다. 두 번째부터는 메시지와 이전 암호화된 문자와의 배타적 논리합을 계산한 후 이를 인코딩하여 암호화된 문자열을 구하고 이를 반복한다.

복호화의 과정 역시 변수들을 초기화시키고 이를 이진수로 변환한다. 마지막 암호화 문자에서 키 값을 디코딩하고, 이를 앞의 암호화 문자와 배타적 논리합을 구하여 원래 메시지를 구하고 이를 반복한다. 첫 번째 문자는 키 값을 디코딩하고 IV와의 배타적 논리합을 통하여 복호화한다.

2.1 암호화 메소드 구현

CBC-MAC의 암호화 메소드는 암호화를 위한 변수를 먼저 초기화 한다. 이때 사용된 변수와 의미는 표 1과 같다.

표1. 암호화에 사용된 변수
Table 1. Variables in encryption method

변수명	의 미
OrginMSG	인코딩될 메시지
IV	초기 벡터
KEY	키
OrginBMSG	인코딩될 메시지 (이진수)
BIV	초기 벡터 (이진수)
BKEY	키 (이진수)
EncBMSG	인코딩된 메시지 (이진수)
Crypto	인코딩된 메시지 (한글자)
Mod	키 문자열 길이

그 다음 먼저 Mod 변수에는 키 문자열의 길이를 저장하여 각 문자의 이진 값과 키의 각 문자의 이진 값의 배타적 논리합을 순서대로 구할 수 있도록 한다.

그리고 OrginBMSG, BIV, BKEY 변수에 각각 인코딩될 메시지, 초기 벡터, 키의 첫 문자를 사용자 정의 메소드인 CharToBinary 메소드를 이용하여 이진수로 변환하여 저장한다. 이때 각각의 문자는 ASCII 값으로 계산하여 구현하였고 이진수 변환 시에는 unsigned char형으로 하여 변환하였다.

메시지 첫 글자를 인코딩하기 위해서는 이진수로 변환된 첫 번째 문자와 IV의 배타적 논리합을 구하고 이 값을 키의 첫 번째 글자의 이진수를 더한다.

두 번째부터는 메시지와 인코딩된 이전 글자와 배타적 논리합을 구하고 인코딩을 하게 된다. 이때 키 값의 길이가 메시지 보다 짧기 때문에 키 문자는 다시 처음으로 돌아와 순환된다. 구체적인 암호화 메소드의 알고리즘은 그림 4와 같다.

```
Encryption () {
        C0 ← IV
        for (i=1 to Message Length)
        { Ci ← E (Pi ⊕ Ci-1) }
        return Encryption Message
}
```

그림 4. 암호화 알고리즘
Fig 4. Encryption algorithm

2.2 복호화 메소드 구현

CBC-MAC의 복호화 메소드는 마찬가지로 변수들을 초기화 하면서 시작한다. 이때 사용된 변수와 의미는 표 2와 같다.

복호화 메소드가 실행되면 암호화 메소드의 역순으로 동작을 하게 된다. 마지막의 암호화된 문자로부터 현재 암호화된 문자의 이진수 값에 키 값의 이진수 값을 빼고 그 값을 앞의 암호화된 문자의 이진수 값과 배타적 논리합 과정을 통하여 원래 메시지를 구할 수 있게 된다.

첫 번째 글자는 암호화 과정과 마찬가지로 초기 벡터 값과의 배타적 논리합을 통하여 구할 수 있게 되고 구체적인 알고리즘은 그림 5와 같다.

Ⅳ. 실험 및 고찰

1. CBC-MAC 알고리즘 검증

본 연구에서는 Microsoft 사의 Visual Studio 2008을 이용하여 구현하였으며 C# 언어를 이용하였다. 또한 블록 암호화에서는 끼워 넣기 (zero padding) 과정이 필요하나 본 논문에서는 ASCII 코드를 이용하므로 (8 bit 고정) 별도의 끼워 넣기 과정이 필요 없다.

표2. 복호화에 사용된 변수
Table 2. Variables in decryption function

변 수 명	의 미
EncBMSG	인코딩된 메시지 (이진수)
DecBMSG	디코딩된 메시지 (이진수)
DecMSG	디코딩된 메시지
IV	초기 벡터
KEY	키
BIV	초기 벡터 (이진수)
BKEY	키 (이진수)
KeyLen	키 문자열 길이
EncMSGLen	인코딩 문자열 길이

```
Decryption () {
        C0 ← IV
        for (i=1 to Message Length)
        { Pi ← D (Ci) ⊕ Ci-1 }
        return Decryption Message
}
```

그림 5. 복호화 알고리즘
Fig 5 Decryption in algorithm

MAC을 만들기 위하여 원래 메시지의 4글자만을 사용하였고, 만약 이보다 짧은 메시지를 전송할 경우 모든 글자를 인증 과정에 사용하게 된다.

그림 6에서 보면 먼저 보낼 메시지를 입력하고 키 값을 설정한다. 실험 시 사용된 키값은 "key"를 사용하게 되고 이 값은 이진화 되어 사용되게 된다.

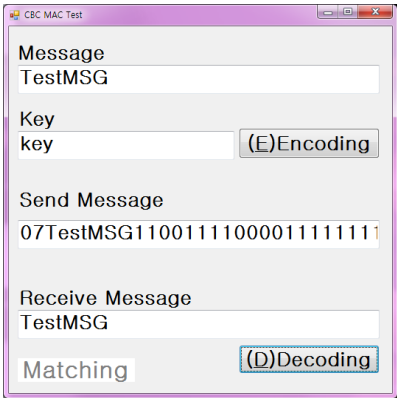


그림 6. CBC-MAC 알고리즘 검증
Fig 6. Verification of CBC-MAC algorithm

그림 6에서 보면 먼저 보낼 메시지를 입력하고 키 값을 설정한다. 실험 시 사용된 키값은 "key"를 사용하게 되고 이 값은 이진화 되어 사용되게 된다. 인코딩을 하게 되면 원 메시지 크기와 원 메시지 그리고 앞의 4글자 "Test"를 암호화하여 이진수로 변환한 값을 보내게 된다.

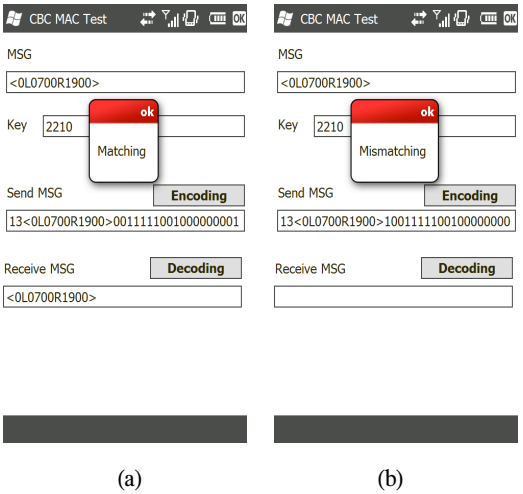
디코딩을 하면 앞의 2자리 숫자를 통해 원래 메시지와 MAC부분을 분리하게 되고 MAC를 복호화 하여 원래 메시지와 비교하게 되며 그림 6에서와 같이 "Matching" 이라는 메시지와 함께 정상적으로 전송되었음을 확인할 수 있었다.

2. CBC-MAC 의 모바일 기기 제어시스템 적용

그림 7 (a) 에서 제어 메시지를 암호화될 메시지로 하고 키 값을 "2210" 문자열로 하여 암호화를 하고 이를 수신측에서 복호화 하여 정상적으로 전송이 되었음을 보여주고 있다.

그림 7 (b) 에서는 MAC 부분에 외부공격에 의한 변형을 가상하여 임의의 한 bit를 추가하여 전송하였는데 복호화가 정상적으로 이루어지지 않음을 보여주고 있다.

제안하는 보안 MIV 시스템이 지원하는 무선 환경은 Wi-Fi (Ad hoc 및 Infrastructure 모드) 및 3G 망이다. 제안 시스템의 검증을 위해 이러한 무선 환경에서 제어메세지에 의한 차량구동 실험을 수행하였다.



(a) (b)

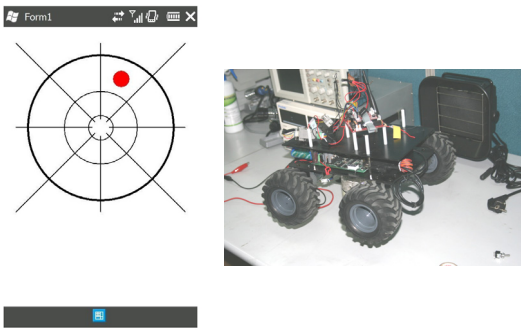
그림 7. CBC-MAC 알고리즘의 MIV 적용
Fig 7. CBC-MAC algorithm applied to a MIV system

차량구동 실험은 그림 8 (a)과 같이 모바일 사용자인터페이스를 구축하였으며 사용자가 터치패드에 입력하면 (그림에서와 같이 특정 방향으로 차량구동 제어) 입력된 위치에 따라 계산된 제어 신호가 암호화된 후 주행로봇에 장착된 ECU (Electronic Control Unit)로 보낸다. 수신한 신호는 복호화를 통해 정상적으로 수신이 이루어졌음을 확인한 후 주행로봇을 구동시킨다. 구현된 하드웨어 MIV 시스템(주행 로봇)은 그림 8 (b)와 같다.

정상적으로 송신을 하였을 경우에는 주행동작이 정상적으로 이루어짐을 확인할 수 있었고, 외부 공격 등에 의한 잘못된 제어 메세지를 수신하였을 경우에는 차량구동이 제대로 동작되지 않음을 확인하였다.

V. 결 론

기존의 모바일기기를 이용한 제어 시스템 구현은 제어 방식에만 치중되어 있어 보안적인 측면에서 MIV의 연구 및 구현이 요구되고 있다. 본 연구에서는 CBC-MAC 인증 알고리즘을 적용해 안전성을 갖춘 개선된 보안 모바일기기 제어시스템을 제안하였다. 인증 알고리즘에 의해 보안 기능이 적용된 MIV 시스템이 정상적으로 동작됨을 확인할 수 있었다.



(a) (b)

그림 8. 모바일 사용자 인터페이스, 구현된 MIV system
Fig 8. Mobile user interface, Development of MIV systeM

참고문헌

[1] 김기영, 강동호, “개방형 모바일 환경에서 스마트폰 보안기술”, 한국정보보호학회, pp. 24-26, 2009
[2] ISO/IEC 9797-1 “Information technology-Security techniques-Message Authentication Codes (MACs) Part1 : Mechanism using a block cipher”, 1999
[3] 곽원숙 외 7명, “CBC-MAC 기반의 위성 관제 신호 보호 알고리즘” 한국통신학회논문지, pp. 616-619, 2002
[4] 마이크로소프트, http://www.microsoft.com
[5] 삼성 모바일, http://www.samsungmobile.com
[6] 박승안, 암호학과 부호이론, 경문사, pp. 60-65, 2003

저자소개

황재영(Jae-young Hwang)

2010년 부경대학교 전자정보통신공학(공학사)
2010년~ 부경대학교 정보통신공학 석사과정
※관심분야 : 모바일 클라우드 컴퓨팅, 이동통신

최동욱(Dong wook Choi)

2005년 부경대학교 전자정보통신공학(공학사)
2009년~ 부경대학교 정보통신공학 석사과정
※관심분야 : 이동통신, 채널코딩

정연호(Yeon-ho Chung)

1992년 The Imperial College, Univ. of ondon, U.K. (공학석사)
1996년 Liverpool University, U.K. (공학박사)
2001년-현재 부경대학교 정보통신공학 부교수
※관심분야 : 적응 변조및 부호화 기술, 반송파 간섭 신호 기술, OFDM, IDMA