The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 14, No. 5, pp.19-26, Oct. 31, 2014. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2014.14.5.19
JIIBC 2014-5-3

기기 간 메시지 부분 암호화 연구

A Study on Efficient Encryption for Message Communication between Devices

이양호*, 신승중**

Yang-Ho Lee*, Seung-Jung Shin**

요 약 최근의 스마트폰의 등장으로 기기간의 역기능들이 속속히 드러나고 있다. 대표적으로 컴퓨터에 의한 정보통신의 역기능을 그 예로 들 수 있다. 또한 갈수록 고도화 되어가는 사이버를 겨냥한 해킹 위협은 그 피해와 파괴력이 점점 확산되고 있어 국가적인 위기로까지 고려해 보아야 할 상황에 이르렀다. 이러한 상황에서 정보기술의 범죄는 사회적인 문제로 볼 수 있다. 인터넷의 발달로 스마트해진 기기뿐 아니라 선박, 비행기, 건물 그리고 자동차에도 디지털화된 기술이 많이 추가됨으로써 해커들의 공격이 가능해 지고 있다. 인간과 인간, 기기들간, 인간과 기기간 모두 사회적 위기로 볼 수 있다. 본 논문에서는 이와 같은 문제를 연구하고자 한다.

Abstract The advent of smart phones brought adverse effect between devices recently. For example, adverse effects of info-communication with advent of computer. Also, hacking threat aiming cyber space that is getting more advanced is spreading in terms of range and danger, so that it reaches the level that the nation has to concern. In this circumstance, crimes involving info-technology is now problem in society. As internet technology advances, it enlarges the range of hacker's threat to not only smart phones, but ships, aircrafts, buildings, and cars. It could be seen as social threat of between human and human, between machine and machine, and between human and machine. This study discuss these problems.

Key Words : Vehicle Network, Wierless Security Protocol, fuggy integral

Ⅰ. 서 론

1. 연구의 배경의 필요성

최근의 스마트폰의 등장으로 기기간의 역기능들이 속속히 드러나고 있다. 대표적으로 컴퓨터에 의한 정보통신의 역기능을 그 예로 들 수 있다. 또한 갈수록 고도화 되어가는 사이버를 겨냥한 해킹 위협은 그 피해와 파괴력이 점점 확산되고 있어 국가적인 위기로까지 고려해 보아야 할 상황에 이르렀다. 이러한 상황에서 정보기술의 범죄는 사회적인 문제로 볼 수 있다.

21세기에는 IT 관련 기기에 스마트화된 플랫폼이 장착되어 모든 업무들이 이를 통해 이루어 질 수 있다.

자동차의 경우 과거 자동차와는 달리 운전자에게 적절한 정보를 제공해 주고, 기기간의 통신을 통해 차량자체가 운전자를 지원하는 지능형 운송수단으로 변화되고 있다.

이와 같이 IT 기술이 적용되는 모든 분야의 다양한 서비스와 편의를 제공해 줌으로써 윤택한 삶을 추구하게

*정회원, (주)한길자동차 종합타운
**정회원, 한세대학교 IT 학부
접수일자 : 2014년 7월 25일, 수정완료 : 2014년 8월 30일
게재확정일자 : 2014년 10월 10일

Received: 25 July, 2014 / Revised: 30 August, 2014
Accepted: 10 October, 2014
**Corresponding Author: expersin@hansei.ac.kr
School of Information Technology, Hansei University, Korea

되었다. 그리고 사용자 뿐만 아니라 기기들 간의 보안의 취약성은 사회적인 위기로 대두되고 있다. 그러나 개방된 네트워크를 통한 악의적인 목적의 사용자 공격수준도 잇따라 향상됨에 따라 공격유형이 보다 다양해지고 지능화되어 그 피해 규모 역시 증가하고 있다. 이러므로 정보통신 기술은 보안적인 책임을 계속 중요시 요구 되고 있다.

하나의 예로 미국의 컴퓨터 보안전문업체 Mcafee사는 인터넷의 발달로 스마트해진 기기뿐 아니라 선박, 비행기, 건물 그리고 자동차에도 디지털화된 기술이 많이 추가됨으로써 해커들의 공격이 가능해 지고 있다.

무엇보다 요즘 차량들은 블루투스나 텔레매틱스(Telematics)기능 등으로 연결돼 있어 원격조작이 가능해졌으며, 최근 자동차가 각종 첨단기기의 장착으로 내부 온도 조절장치나 자동주차 및 충돌방지장치 등 관련 컴퓨터 시스템 기기가 70가지에 육박하게 됨으로써 부각되기 시작한 문제점이라 밝혔다. 그래서 인간과 인간, 기기들간, 인간과 기기간 모두 사회적 위기로 볼 수 있다. 본 논문에서는 이와 같은 문제를 연구하고자 한다.

2. 연구의 방법

기기들 간의 통신 네트워크에 의해 발생되는 테이터와 인간과 기기들 간에 사용되는 테이터들을 해킹을 한다면 위기 및 문제가 발생되므로 자동차 기기간의 이론적 연구가 필요하다.

위기관리에 대한 우리나라의 관심은 해마다 발생하는 자연재해를 중심으로 1990년대 초기부터 부각되기 시작하였다. 그 이후 1990년대 중반 이후에는 인위재난에 의한 재해가 지속적으로 발생하여 그 피해 규모가 광범위해 지자 위기관리의 대상은 점차 자연재난에서 인위재난으로 관심이 기울어지게 되었다. 그로 인해 1990년대 중반 이후에는 여러 학자들에 의해 인위재난 관리전략과 정책에 대한 연구가 그 주를 이루었다.

그러나 인위재난 관리전략을 위한 노력에도 불구하고 발전하는 과학기술에 의한 새로운 인위적 유형의 재난에 적절하게 대처하지 못한다는 지적을 받기도 하였다. 급변하게 발전하는 정보통신기술과 인터넷 구축의 기반으로 사이버관리체제에서 모든 업무가 이러한 IT환경에서 이루어지고 있다. “최근 이동통신기술의 발전으로 정보화시대로 나아감에 있어 국가위기관리차원에서 사이버안보를 확보하는 것만큼이나 시급하고 절박한 과제는 없을 것이며, 21세기 선진 사이버위기관리 시스템 체계를 구축하여 관련 대응방안을 모색하는 것 또한 매우 중요한 과제”라 보았다. 그런가하면 이필재(2009)의 유비쿼터스 환경과 국가사이버위기관리 법·제도의 문제점 및 개선방안에 의하면 “사이버공격으로 초래되는 사이버상의 위기는 현실세계의 물리적 혼란과는 달리 특정 개인에 관한 것일지 라도 국가 전체의 위기로까지 확대될 수 있으며,무엇보다 유비쿼터스 환경의 경우엔 사이버 공간과 물리적 공간의 융합체제이기 때문에 사이버공간에서의 혼란은 바로 물리적 공간의 혼란으로 직결될 수 있다”고 보았다.

II. 관련 지식

1. 자동차 통신네트워크의 개념

자동차 통신네트워크의 등장 계기는 ECU(Electronic Control Unit; 전자 제어시스템, 이하 ‘ECU’라 칭함) 기술에 의해서이다. 자동차에 전자제어 시스템이 처음으로 도입된 시기는 1988년도로 1986년 보쉬(Bosch)사에서 개발한 자동차용 통신네트워크 시스템인 CAN(Controller Area Network; 계측제어통신망, 이하 ‘CAN’이라 칭함)에 의해서이다.

CAN은 차량용 통신네트워크 시스템으로 기존 자동차 부품들이 유선으로 모두 연결되어 있던 점을 무선통신방식으로 연결하여 수많은 연결선을 제거함으로써 결국 자동차의 무게가 감소하게 되어 연비가 절감되고, 배기가스의 검출 또한 대폭 감소시켜 주는 계기가 되었다. 결과적으로 자동차의 성능을 대폭 상승시키는 역할을 한 셈이다.

이러한 차량통신 네트워크는 내부망과 외부망으로 구분되는데, 차량 내부망은 IVN(InVehicle Network; 내부통신네트워크, 이하 ‘IVN’이라 칭함)라 부르며, 차량 외부망은 VANET(Vehicular Ad-hoc Network; 외부통신네트 워크, ‘VANET’라 칭함)라 일컫는다. 차량의 내부통신네트워크인 IVN은 차량 내 센서나 전자장치 디바이스(Device)간 이어주는 유·무선 통신네트워크 역할과 함께 자동차 전자제어시스템으로 제어정보데이터를 보내는일을 한다. 이러한 IVN은 차량의 개인편의 및 안전서비스 지원을 위한 유선통신 네트워크와 멀티미디어 서비스 지원을 위한 무선통신네트워크로 분류된다.

IVN에 해당하는 통신네트워크로는 차량의 바디나 미

터 ·엔진 부분을 연결하고 제어하는 CAN, 차량의 내비게이션이나 오디오 ·앰프 ·CDP 등의 멀티미디어 기기 접속을 연결하는 MOST(Media Oriented System Transport; 차량 네트워크시스템, 이하 'MOST'라 칭함), 엔진 및 브레이크나 조향장치를 연결하고 제어하는 Flex Ray(전기신호제어장치),바디계의 도어 미러나 윈도우를 제어하는 LIN(Local Interconnect Network; 근거리 연결 통신망, 이하 'LIN'이라 칭함), 오디오나 차량용 카메라 등을 연결하고 제어하는 IDB-1394(ITS Data Bus-1394; 지능형 교통시스템 인터페이스, 이하 'IDB-1394'라 칭함)가 있다.[7][8]

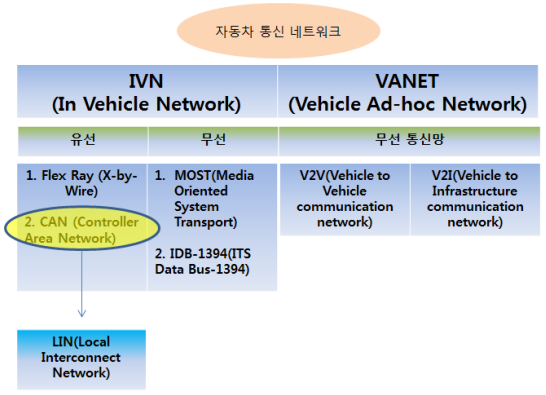

그림 1. 자동차 통신네트워크 구조체계
Fig. 1. vehicle network structure system

2. CAN(ControllerAreaNetwork)

CAN은 자동차 내 컨트롤러와 센서 ·액추에이터(Actuator)·ABS(Anti lock Brake System)·오디오 시스템,블루투스 ·전자제어시스템 등을 연결하기 위해 개발된 시리얼 통신 프로토콜로 높은 데이터 전송률과 함께 다수의 전자제어장치를 상호 연결하여 실시간으로 제어함으로써 효율적으로 여러 노드(Node)를 지원하는 분산 제어 네트워크이다. 이 중에서도 CAN에서의 블루투스 서비스 지원은 CAN 컨트롤러와 데이터의 송수신을 위한 연동서비스에 의해 가능하다.

즉, 차량의 진단과 유지관리, 도난방지나 사고처리 등의 서비스는 텔레매틱스 소프트웨어 플랫폼에 의해 기술구현이 가능한데, CAN 드라이버와 액서스 스택에 의해 블루투스와 USB 드라이버 스택구현이 가능하며, PCI인터페이스에 의한 시리얼과 USB의 인터페이스가 가능하다.[6]

CAN은 고속과 저속으로 분류되는데, 고속 CAN은 엔진제어(Engine Control) · ABS·브레이크 · 전송제어(Transmission Control) · 능동적 서스펜션(Active Suspension)기능을 데이터 전송률 1Mbps속도로 제어하며, 저속 CAN는 라이팅 · 에어컨 · 파워윈도우 · 에어백 · 파워락 · 파워시트 기능을 데이터 전송률 125Kbps 속도로 제어한다.

CAN 통신규격은 메시지에 있는 식별자인 ID(Identifier; 사용자식별부호, 이하 'ID'라 칭함)의 길이에 따라 두 가지 모드로 구분되는데, 같은 동급버전으로부터 보내온 메시지만 받아들이는 표준 CAN(버전 2.0A,11Bit식별자)과 CAN 2.0A와 CAN 2.0B Controller에서 보내온 메시지 모두를 받아들이는 확장 CAN(버전 2.0B, 29Bit 식별자)으로 나누어지며, CAN 프로토콜(Protocol)프레임의 형태는 총 4가지로 분류 및 정의되어지는데, 데이터 전송기능을 담당하는 DataFrame, 데이터 프레임의 전송요구를 담당하는 RemoteFrame, 지역적으로 감지된 에러의 전역적인 신호역할을 담당하는 ErrorFrame, 데이터 프레임과 리모트 프레임들의 앞 ·뒤에서 메시지간의 전송간격조절을 하는 Overload Frame로 분류된다.[10]

CAN 통신 동작원리는 Ethernet과 유사하다. 전송데이터 메시지의 내용에 따라 아이디를 부여하여 모든 메시지를 구별하고, 메시지를 최우선으로 정하는 내용에 의해 주소지정을 하게 된다. 수신 상태의 스테이션들은 수신된 메시지의 ID를 판독하여 수신된 데이터의 관련유 ·무를 확인 후 관련이 있으면 데이터를 받아들이고 관련이 없으면 무시하는 체계를 지니고 있다. 만약 두 개 이상의 스테이션이 동시에 데이터를 전송하였을 경우 충돌하는 메시지의 아이디를 한 Bit씩 비교하여 가장 높은 우선순위를 가진 메시지만 전송을 계속하고, 나머지 메시지는 즉시 전송을 중단하게 된다.

이러한 CAN은 자동차 네트워크 분야에서만 아니라 철도나 선박, 의료, 산업네트워크 분야에까지 다양하게 적용하고 있으며, CAN 확장 규약을 제정하여 비행기나 제트기의 조종석과 항법장비에까지 널리 쓰이고 있는 것으로 알려져 있다.

CAN 통신방식은 CSMA(CarrierSense Multiple Access;반송파감지다중 액서스, 이하 'CSMA'라 칭함)방식으로 버스에 연결된 노드가 데이터를 전송하기 위해서는 기존의 전송데이터가 없을 때까지 기다려야 하기에 전송지연 결과를 초래할 수 있는 단점을 지니고 있는 반

면 Flex Ray는 TDMA(Time Division Multiple Access; 시분할 다원접속, 이하 'TDMA'라 칭함) 방식으로 동작한다(박상현 등, 2009, p.303). 이는 버스에 연결된 시스템들은 독점적으로 진입권한이 허용되는 고정된 시간슬롯(Slot)을 할당받게 된다.[1] 시간 슬롯들은 정의된 간격으로 반복되어 데이터가 버스상에있는 시간을 정확히 계산하여 버스진입이 가능하게 해주는 역할을 한다.특히 운전자의 실제 주행과 관련된 브레이크의 경우 기기의 조작을 수행하였을 때 해당 컨트롤 신호가 정해진 시간 내에 목적지로 전송되는 것이 반드시 안정적으로 신뢰되어야 하는데, Flex Ray는 메시지의 버스진입과 전송시간이 정확한 동작 안전성이 보장되어야 하는 운전자의 생명과 직결된 통신네트워크라 할 수 있다.[9]

Ⅲ. SM^{2}P 제안 모델

1. 자동차 네트워크 정보보호 서비스

본 논문에서는 정보의 기밀성을 보장하는 시스템제어장치(MCU)와 전자제어장치(ECU)간 메시지 전송 보안 모델을 제안한다. 제안하는 모델에서 메시지의 기밀성 보장과 인증 보장을 위해 이중 XOR 암호화를 이용하여 송수신부간 메시지를 교환하고, 제어 메시지에 대한 인증처리를 위해 초기화 벡터(IV)와 원타임패스워드(OPT)을 사용하였다. 이때 보안 네트워크에서는 단일 XOR 암호화 알고리즘을 적용하는 기존 SEA모델과는 달리 이중 XOR연산을 사용하는 보안메시지 전송 모델인 안전한 자동차 메시지전송 모델(SM2P)을 제안하고 이를 사용한 디바이스간 메시지 전송을 방법을 사용한다.

자동차 네트워크에서 정보보호 서비스를 제공하기 위한 필요요소로는 첫째, 메시지의 기밀성과 무결성의 확보이다. 이 중 인가되지 않은 자의 임의적 수정의 기반이 되는 노출을 방지하기 위해서는 기밀성의 확보가 우선되어야 한다. 기밀성의 확보를 위해 본 연구에서는 메시지 암호화를 사용하고 무결성 확보를 위해 디지털 서명을 적용한다. 두 번째 요소로는 실시간성의 보장이다. 실시간성의 보장은 제어메시지의 정상적인 도달을 보장하는 것 만큼 중요한데, 빠른 반응속도가 필요한 자동차 네트워크에서는 더욱 필요하다고 볼 수 있겠다. 하지만 첫 번째 필요오소인 기밀성과 무결성 확보를 위해 암호화를 적용할 경우 두 번째 요소인 실시간 성 보장이 힘들어진다. 본 논문에서는 이중 XOR 암호화를 적용하여 이 두 가지 상반된 문제점을 해결한다.

이중 XOR 암호화 기법은 송수신부의 부하를 줄일 수 있으며 제어처리 속도를 향상시킬 수 있다. 또한 IV와 OPT를 통한 암호화를 수행하여복호화에 소요되는 처리시간을 감소시킬 수 있다. 이중 XOR 암호화를 수행할 때 비밀키와 공개키 암호화 방법은 제어데이터에 대한 암호화의 수행에 처리속도가 지연되어 실시간 제어정보가 필요한 경우에는 부적절한 방법이 된다. 이에 따라 메시지를 XOR 연산 후 암호화해 수신부에서 인증할 수 있도록 IV와 OPT를 동기화 시켜 전송하는 방법이 필요하다. 즉, 네트워크 통신은 인증을 위하여 중간 중개자를 가질 필요가 없고 비밀키나 공개키를 사용하지 않는 디바이스간 보안이 반드시 필요하다.

단순 XOR 암호화 기법에서 키값인 OPT와 평문 메시지를 입력으로 XOR암호화하게 된다. 그러나 이 상태로 메시지를 송수신부간 교환하게 되면데이터 보호에 문제가 발생 할 수 있다. 즉 기밀성에 문제가 발생될 수 있다. 디바이스간 전송되는 메시지의 포맷은 제한되어 있어 이의 추론이 가능하고 교환되는 메시지는 제3자에게 노출될 가능성이 존재한다.

전송 메시지의 안전한 전달을 위해 송수신부에서 수행되는 이중XOR 연산은 인증과 메시지를 훼손하는 것을 방지한다. 메시지 전송을 위한 보안 네트워크를 구성하는 송수신부는 메시지의 기밀정보를 이중 XOR 암호화를 사용하여 제3자는 볼수 없어야 한다. 전송되는 메시지는 OPT와 IV를 이용하여 인증을 제공하고 기밀성 제공을 위해 사용하는 알고리즘은 이중 XOR알고리즘을 사용한다.

실제 적용되는 방법은 기밀 유지가 필요한 메시지를 보안토큰과의 XOR 연산 방법을 사용한다. 일반적으로 통신 네트워크에서 사용하는 방법인 단일 XOR 암호화하고 암호화된 메시지를 XOR연산 한다면 나중에 메시지의 포의 종류가 한정되어 있어 XOR연산 대상인 메시지를 추론할 수 있어 보안 위협이 될 수 있다.

현재 네트워크로 어떤 데이터를 전송할 때 범용적인 메시지 전송 보안 프로토콜을 사용하여 데이터의 기밀성을 보장할 수 있다. 이에 따라 메시지에 XOR르르 이중 연산해 전송함으로써 메시지의 추론을 불가능하게 하고 인증하도록 함으로써 송수신자간 안전한 메시지 교환 기법을 사용한다.

네트워크 계층에서의 보안은 주고 받는 메시지에 대해서 단일 XOR 암호화와 복호화를 수행하는 경우에 보안에 취약하고 메시지 추론에 취약함으로써 자동차 제어 장치의 보안에 큰 위협이 될 수 있다. 제어 시스템에서 단일 XOR연산의 사용은 송수신부 간의 메시지의 추론 가능성을 확대함으로써 보안성과 신뢰성이 완전히 보장되지 않는 문제점도 가지고 있다.

이런 면에서 보안이 필요한 메시지에 대해서 이중 XOR알고리즘을 적용해 송수신자간에 보안서비스를 해주는 보안기법이 필요하다. 한쪽에서 다른 한쪽으로 데이터를 보낼 때 중간매개자(intermediaries)없이 직접적으로 신뢰된 채널을 통해 데이터를 전송하는 방법을 적용한다. 이 모델에서는 응용계층의 보안프로토콜을 이용하여 구축하는 것이 일반적이다.

본 논문에서는 단일 XOR보안알고리즘을 적용하는 대신 메시지와 키를 암호화하기 위해서 이중 XOR알고리즘을 적용하였다. 이중 XOR암호화는 송수신자간 메시지 전송 프로토콜을 사용하는 네트워크를 구성하는 수신부에서 송신부로 보낸 메시지에 대한 인증과 암호화가 필요하다. 송수신부에서는 메시지를 인증과 동시에 복호화하여 정보를 저장한다.

2. 네트워크 통신의 연구 모델

메시지 포맷은 메시지의 논리구조와 내용을 기술하기 위한 것으로 네트워크에서 구조화된 메시지를 전송가능하도록 설계된 표준화된 형식이다. 메시지 포맷을 이용하면 메시지의 내용이나 내용 구조를 정의할 수 있고 다양한 응용들 사이에 구조화된 메시지를 상호교환 할 수 있다.

메시지 포맷을 분석하는 파서는 다양한 유형의 코드를 지원한다. SXP 무선 보안 프로토콜의 응용구조는 그림 2와 같다.

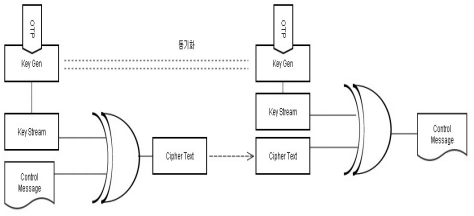

그림 2. SXP 무선 보안 프로토콜의 응용구조
Fig. 2. Application Structure of SXP Wierless Security Protocol

자동차의 특수한 상황으로 인해 전송되는 메시지가 동일하거나 메시지 풀(pool)이 제한적이기때문에 전송되는 암호화된 메시지를 중간에서 가로채는 경우에 XOR 연산자의 취약점으로 인해 메시지의 내용을 유출할 수 있는 가능성이 제기된다. 각 장치마다 제조번호나 차대번호 등 일련번호를 가지고 있다. Initial Value 를 통신제어 메시지와 XOR하여 통신제어 메시지를 다른 형태로 변환하여 이를 키스트림(Key Stream)과 XOR하여 암호화 메시지를 생성한다. 자동차가 생산되는 시점에서 주어지는 Initial Value 값이므로 이는 외부로 유출되지 않는 정보라고 가정하였을 경우, 수신된 통시 메시지의 인증 기능이 가능하다.

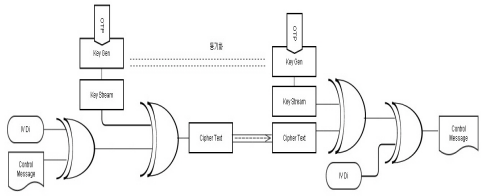

그림 3. SM²P 무선 보안 프로토콜의 응용구조
Fig. 3. Application Structure of SM²P Wierless Security Protocol

Ⅳ. SM²P의 프로토콜 검증

1. 프로토콜 검증

프로토콜의 평가 모델은 미래의 자동차 환경 하에서 적용할 SM²P 시스템과 SXP 시스템의 비교우위를 검증하기 위하여 수학적 모델링과 계층퍼지적분을 사용하였다.[2]

수학적 모델링은 비교 프로토콜인 SXP와 제안 프로토콜 SM²P에서 사용된 OPT와 IV를 입력으로 하는 XOR연산을 이용해 암복호화 하는 실행 프로토콜을 대상으로 도출하였다. SXP 실행 프로토콜은 그림 과 같이 표현할 수 있는 반면 SM²P 실행 프로토콜은 그림 과 같이 이중 XOR연산을 적용하고 있다. SXP와 SM²P의 보안연산 프로세스의 수학적 검증 모델은 그림 4과 그림 5로 표현된다.[5]

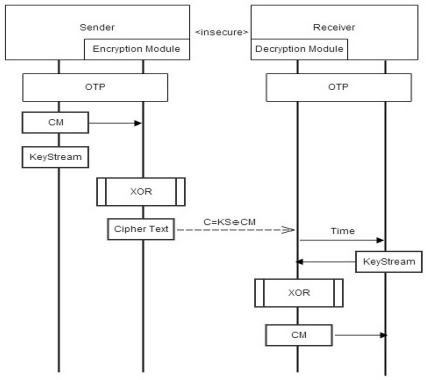

그림 4. SXP 실행 프로토콜
Fig. 4. SXP Execution Protocol

Step 1: 송신자와 수신자간의 키교환없이 암호화키로 OTP를 사용하기 위해 시간 기반의 동기화가 필요하다.

Step 2: 송신자는 전송메시지인 제어메시지(CM)를 암호화하기 위해 먼저 키스트림을 생성해야 한다. 송신자가 가지고 있는 OTP를 이용하여 키스트림함수(K)에 의해 키스트림을 생성한다.

Step 3: 실시간스트림암호알고리즘, 즉 XOR 연산자를 이용하여 암호문(C)을 생성한다. 암호문은 제어메시지(CM)와 키스트림을 XOR 연산자로 계산하여 생성한다.

Step 4: 송신자는 암호화모듈을 통해 생성된 암호문(C)를 수신자에게 전달한다. 안전하지 않은 채널을 통해 전송되기 때문에 공격자로부터 도청이 가능하다.

Step 5: 수신자는 복호화 모듈을 통해 암호문이 전송되었음을 확인할 수 있다. 복호화를 위해서는 키스트림을 생성해야 하는데 이때 OTP 값이 필요하다. OTP는 시간에 의해 수시로 변경되기 때문에 키스트림이 생성된 시간이 필요하다.

Step 6: 수신자는 주어진 시간을 근거로 OTP 값을 도출하여 OTP 값을 입력값으로 키스트림을 생성한다.

Step 7: 생성된 키스트림과 암호문을 XOR연산하여 송신자가 보내고자 했던 제어메시지로 복호화한다.

Step 8: 복호화된 제어메시지(CM)를 수신자는 확인하고, 제어메시지에 맞게 제어시스템을 조정한다.[3]

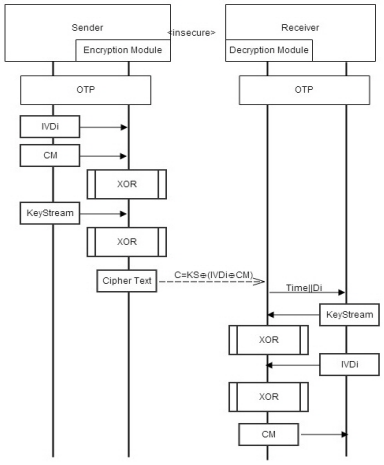

그림 5. SM^{2}P 실행 프로토콜
Fig. 5. SM^{2}P Execution Protocol

Step 1: 송신자와 수신자간의 키교환없이 암호화키로 OTP를 사용하기 위해 시간 기반의 동기화가 필요하다.

Step 2: 장치마다 식별이 가능한 정보(IV_{D_i} : Initial Value)를 가지고 있다. 이 정보는 계산하는 과정에서만 사용되고, 전송하지 않는 비밀정보이다. 초기설정값을 통해 장치의 인증하기 위해 공격자로부터 보호가 필요한 정보이다. 제어 메시지(CM)를 알아 볼 수 없는 정보로 가공하기 위해 각 장치의 초기설정값(IV_{D_i})가 필요하다.

Step 3: 제어 메시지를 가공하기 위해 송신자의 초기설정값(IV_{D_i})과 제어메시지를 XOR연산하여 전처리암호문(C_0)을 생성한다. 이는 송수신간의 제어메시지의 제한적인 풀(pool)을 확대하는 효과가 있어 같은 제어메시지라도 매번 다른 암호문으로 생성되는 효과를 가지게 된다. 공격자는 예상 가능한 제어 메시지를 예측하기 어렵다.

Step 4: 수신자에게 보내질 최종암호화를 하기 위해 스트림암호알고리즘을 사용한다. 스트림 암호 생성을 위해 키스트림(KeyStream) 생성이 필요하다. OTP를 입력으로 하는 함수(K)를 통해 키스트림을 생성한다.

Step 5: Step3에서 생성된 전처리암호문

($C_0 = CM \oplus IV_{D_i}$)를 키스트림과 XOR 연산을 하여 수신자에게 보낼 암호문을 생성한다.

Step 6: 송신자는 생성된 암호문(C)을 수신자에게 전달한다. 안전하지 않은 채널을 통해 전송되기 때문에 공격자는 전달되는 암호문 도청이 가능하다.

Step 7: 사전 동기화된 OTP 값을 생성하기 위해 수신자는 OTP 생성시간을 알아야 한다. 복호화하는 과정에서 송신자의 식별정보인 초기설정값이 필요하기때문에 암호문을 보낸 송신자를 확인이 필요하다.

Step 8: 수신받은 암호문을 복호화하기 위해 OTP를 생성하여 OTP를 입력값으로 키스트림을 생성한다.

Step 9: 주어진 암호문과 키스트림을 XOR 연산을 하면 XOR연산자의 결합법칙에 의해 전처리암호문($C_0 = CM \oplus IV_{D_i}$)을 생성된다.

Step 10: 송신자와 수신자은 사전에 각 장치의 초기설정값(IV_{D_i})을 가지고 있다. 이 정보는 송신자의 발신자인증을 확인할 수 있는 정보로 활용된다.

Step 11: 송신자의 초기설정값(IV_{D_i})을 이용하여 복호화하여 제어메시지를 도출한다.

Step 12: 복호화알고리즘을 통해 제어메시지를 도출하고, 도출된 제어메시지를 수신자는 확인하고 메시지에 따라 제어시스템을 동작한다.[4]

2. 계층 퍼지적분 평가 알고리즘

평가 대상 문제가 여러 개의 항목으로 구성된 계층구조로 주어져 있을 경우에 계층 퍼지적분 알고리즘은 다음과 같이 정리할 수 있고 [그림 6]과 같이 표현된다.

단계 1 : 평가대상의 항목을 계층화하여 평가항목의 중요도(μ) 및 평가항목간의 상호작용계수(λ)를 조사한다.

단계 2 : 평가항목간의 중요도 및 평가항목간의 상호작용계수를 이용하여 퍼지측도(g(・))를 구한다.

단계 3 : 자료 또는 평가에 의해 평가 대상에 대한 평가항목별 평가치 h(・)를 구한다.

단계 4 : 최하위 계층에서는 평가항목별 평가치 h(・)와 g(・)를 사용하여 퍼지계층 적분으로 통합평가를 하며 그 이외의 계층에서는 단순가중법에 의해 통합평가를 행한다.

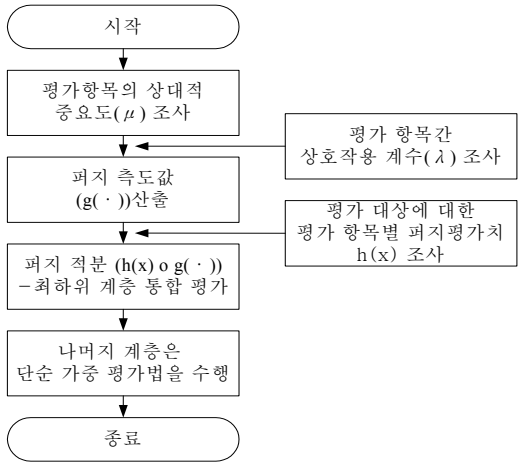

그림 6. 퍼지적분 평가 알고리즘
Fig. 6. fuggy integral Evaluation algorithm

V. 결 론

SM²P와 SXP에 대한 함수 h의 퍼지척도 g에 대한 수게노의 퍼지적분값을 분석해 보면 점수 환산에 의한 부분집합으로 분류된 각각의 영역에서 SXP와 SM²P시스템의 평가치가 거의 차이가 나지 않으나 SM²P는 무결성이 SXP는 기밀성에서 약간 우세하게 평가되고 있음을 확인 할 수 있다. SM²P는 실시간 제어메시지의 인증과 기밀성이 필요한 프로토콜을 요구하는 자동차 시스템의 메시지 보안 시스템으로 적합하다.

표 1. 퍼지적분 결과
Table 1. Integration of Fuzzy

부분집합의 수	측도치 g(・)	SXP h(・)	SM²P h(・)	SXP 평가치	SM²P 평가치
1	0.0589	0.0683	0.0695		
2	0.0576	0.0680	0.0692		
3	0.0550	0.0669	0.0682		
4	0.0590	0.0684	0.0696		
5	0.0520	0.0660	0.0674		
6	0.0649	0.0703	0.0713		
7	0.0614	0.0688	0.0700	0.0682	0.0694
8	0.0571	0.0680	0.0691		
9	0.0532	0.0663	0.0677		
10	0.0587	0.0680	0.0693		
11	0.0470	0.0645	0.0660		
12	0.0707	0.0727	0.0733		
13	0.0703	0.0700	0.0710		

References

[1] JeongHoon Park, Chan-Woo Moon, "Design and Implementtation of a FlexRay-CAN gateway for Real-Time Control", The Journal of the Institute of Internet, Broadcasting and Communication, Vol.14, No.2, pp.53-58, 2014

[2] Dea Su Kim, Soon Cheol Baeg, Kwang Lo Lee, Young Whan Lim, Design and Analysis of Fussy-Expert System Model utilizing Fuzzy Cognitive Maps, PRICAI'92, Sept. 1992.

[3] J. Caballero, H. Yin, Z. Liang and D. Song, "Polyglot: Automatic Extraction of Protocol Message Format using Dynamic Binary Analysis," CCS 2007 Proceeding of the 14th Conference on Computer and Communication Security, ACM, p. 1(15), Sep, 2007.

[4] W. Cui, J. Kannan and H. J. Wang, "Discoverer: Automatic Protocol Reverse Engineering from Network Traces," USENIX Security 2007 Proceeding of the 16th USENIX Security Symposium, USENIX, p. 1(15), Aug, 2007.

[5] Z. Lin, X. Jiang, D. Xu, and X. Zhang, "Automatic Protocol Format Reverse Engineering through Context-Aware Monitored Execution," NDSS 2008 Proceeding of the 15th Annual Network and Distributed System Security Symposium, INTERNET SOCIETY, p. (17), Feb, 2008.

[6] R.Makowitz, and C. Temple, "A communication network for automotive control systems," IEEE 2006 International Workshop on Factory Communication Systems, pp. 207-212, June 2006.

[7] K. Akkaya and M. Younis, "A Survey on Routing Protocols for Wireless Sensor Networks," Ad Hoc Networks, Vol.3 No.5, pp.352-349, 2005.

[8] F. Xiangning, S. Yulin, "Improvement on LEACH Protocol of Wireless Sensor Network", International Conference on Sensor Technologies and Applications, IEEE, pp.260-264, 2007.

[9] Robert I. Davis, Alan Burns, "Robust priority assignment for message on Controller Area Network(CAN)", 26 November 2008. Springer Science Business Media, LLC 2008.

[10] Seung-Hyun Yang, Suk-Won Lee, "A Study of Vehicle's Sensor Signal Monitoring and Control Using Zigbee Wireless Communication and Web-based Embedded System", KAIS, Vol.10 No.1, pp.352-349, Jan 2009.

저자 소개

이 양 호(정회원)

- 1975년 : 자동차 정비기능사1급 취득
- 2009년 : 연세대학교 행정대학원 졸업 (정치학석사)
- 2013년 : 상명대 일반대학원 박사과정 수료(한국정치경제학전공)
- 한세대 일반대학원 IT융합학과 졸업 (IT융합 공학박사)
- 2011년 ~ 2013년 서울특별시 강서구 시설관리공단 이사장
- 현재 : ㈜한길자동차 종합타운 회장

<전공분야 : 자동차 보안>

신 승 중(정회원)

- 1988년 : 세종대 대학원 경영학과 졸업
- 1994년 : 건국대 대학원 전자계산학과 졸업
- 2000년 : 국민대 대학원 정보관리 학과 졸업
- 현재 : 한세대학교 IT학부 교수.

<주관심분야 : 정보관리, 정보전, 정보보호, 정보융합관리>