韓國 컴퓨터情報學會 論文誌
第9卷 第1號, 2004. 3.

2004-9-1-2-2

빌딩 출입 보안 시스템의 정보폭주 방지방법에 관한 연구

서 창 옥*, 김 계 국**

A study on a preventive measure of traffic congestion in building security system

Chang Ok Seo *, Kye Kook Kim **

요 약

일반적으로 출입자 정보는 보안서버에서 관리되며, 출입자가 출입카드를 카드리더에 접촉시킬 때 보안서버는 데이터베이스를 검색한 후 출입허용여부를 판단하게 된다. 그런데 많은 출입자가 여러 출입문에서 동시 다발 적으로 카드리더에 출입카드를 근접시키면 정보폭주 가 야기된다. 따라서 서버의 과부화로 인해 출입 지연이 생긴다. 본 논문에서는 정보폭주를 근본적으로 막을 수 있는 구역식별알고리즘을 제안하였다.

Abstract

In general, security server controls information of people who usually come to building. In order to exit and entrance, while they bring IDentification card into contact with card reader, server admits them into building after asks whether their informations are or not in database.

However if many people want to exit and entrance in all direction, it may give rise to a serious traffic congestion. Therefore the delay is due to server's overload. In this paper, we suggested IZA(Identification Zone Algorithm) in order to prevent of traffic congestion.

▸ Keyword : 보안서버, 정보폭주, 구역식별알고리즘

* 건국대학교 대학원 박사수료
** 국립원주대학 전자통신과 교수

Ⅰ. 서 론

요즘 들어 고층화된 빌딩이 많아지고, 그 빌딩에는 다양한 사람들의 출입이 빈번하게 일어나고 있다. 복잡한 빌딩 안의 제어를 담당하는 IBS(Intelligent Building System)는 이 빌딩의 발전과 함께 계속 성장해오고 있었다.

층화된 빌딩을 모두 제어하기 위해 매우 복잡한 구조를 가지고 있으며 요즘 들어 모듈화 간소화가 이루어져 안정성도 높아지고 있다.

이 간소화된 IBS에 빌딩 출입 보안 시스템를 결합하여 통합관리 하는 것이 근래의 추세이다.

출입통제는 RS232C RS485 RS422등의 통신 신호를 사용해 오다, TCP/IP로 바뀌어 가는 추세이다.

빌딩 안에서는 보통 사설IP를 사용하게 되며 전역IP를 사용할 경우에는 보안성의 문제로 인해 암호화 알고리즘을 빌딩 출입 보안 시스템와 결합시켜 보안성을 높여야 한다.[6]

본 논문에서는 전역IP를 사용하지 않고 사설IP를 사용하여 시스템을 구성하였다.

전역 IP를 사용하는 빌딩 출입 보안 시스템은 사설IP 알고리즘에 보안 알고리즘을 강화함으로써 해결 할 수 있다.

보통 TCP/IP를 사용하는 경우 폭주로 인한 시스템 제어권 상실이 일어날 수 있다. 이 또한 다른 통신 방식에서도 폭주로 인한 시스템의 제어권을 상실 할 수 있음을 알 수 있다.[1]

출입하고자 하는 사람이 출입문 센서GS(Gate sensor)에 출입자카드(IDentification Card)를 근접하면 출입자카드번호가 TCP를 통해 출입보안서버의 데이터베이스를 검색하여 출입가능여부를 출입문제어장치 GC(Gate controller)에 알려 출입문을 개방(Open Gate)하게 된다.

만약 불특정다수가 같은 시간에 서로 다른 여러 개의 출입문센서인 GS에 출입자카드를 근접시켰을 경우 각각의 GS에서 동시에 출입 보안 서버에 TCP로 데이터를 보내게 된다. 이때 출입 보안 서버에 들어오는 데이터 순차대로 데이터베이스를 검색하여 그의 응답을 게이트 콘트롤러인 GC에 전송한후 다음 GS에서 들어온 데이터를 분석하여 들어온 GC에 재 응답을 보내게 된다.

서로 다른 출입문에서 동시다발적으로 출입자 카드를 GS에 접근할 때 GS에서 발생된 데이터들이 GC에 전달될 때까지의 시간지연이 매우 커지게 되어 다음 출입자가 인증을 요구할 때 즉시 응답을 줄 수 없게 되고, 이런 악순환으로 인해 시스템 및 네트워크상의 과부화로 인한 정보폭주현상(Congestion of traffi)이 일어난다.

이를 근본적으로 해결하기 위해 각각의 GS 및 GC를 관리 할 수 있는 ESC(Entrance Sensor and Controller)를 두어야 한다.

ESC는 1개의 출입문을 관리할 수 있으며 여러 개 또는 한 개의 GS와 GC를 가 질수 있다.

이 ESC에 출입자 정보를 가지고 있게 하여 출입 보안서버에 접근하지 않아도 출입의 허용여부를 결정 할 수 있는 기능을 가지게 하였다.[5]

이렇게 함으로써 여러 곳에서 동시 다발 적으로 일어나는 출입 제어를 정보 폭주 없이 관리 할 수 있게 된다.

본 논문에서는 AIBS(Advanced Intelligent Building System)에 지역그룹준위(AGLA : Area Group Level Algorithm)를 이용했으며, ESC에 출입자 정보를 효과적으로 배열하기 위해 구역식별알고리즘(IZA : Identification Zone Algorithm)을 제안 하였다.[1]

Ⅱ. AIBS 구성

각가의 출입문에 설치된 ESC에 TCP/IP를 연결한다. 이 ESC-TCP/IP를 스위칭허브를 통해 출입보안 서버에 접속시킨다(그림 1).

각 출입문에 설치된 ESC-TCP/IP를 출입보안서버에서는 폴링(Polling)에 의해 각각의 출입문 상태를 확인하며 각각의 출입문 번호에 해당하는 센서들의 상태를 순서적으로 증가해가며 하나씩 상태를 확인한다.

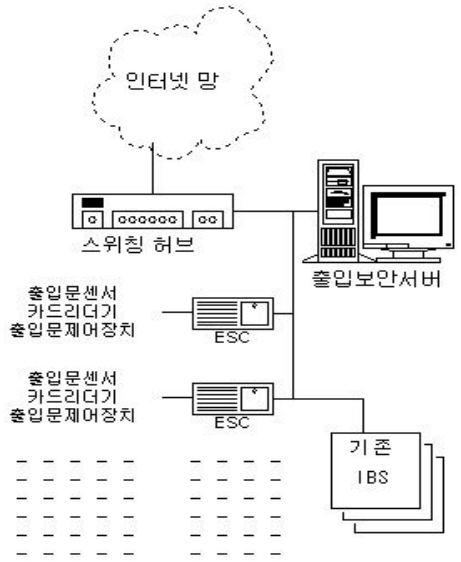


그림 2. AIBS 구성

상태응답이 없을 때에는 3회에 걸쳐 재 전송을 하여 상태요구를 하며 그래도 응답이 없으면 출입보안 시스템에서 ESC의 에러를 관리자에게 즉시 알리게 된다.

이때 출입자카드의 상태를 받기 위한 폴링명령은 "GetCard"이며 출입용 카드 데이터 포맷은 1byte의 STX와 7byte 의 출입자카드번호 1byte의 BCC, 1byte의 ETX로 구성되어 있다.

출입용에 사용되는 출입자카드번호는 RF카드 스마트카드등의 종류가 있는데, 비접촉형 카드인 RF카드를 주로 사용한다. 요즘은 스마트 카드도 비접촉형이 생산되고 있으므로 많이 사용하는 추세이다.

ESC에서 GetCard명령에 의해 출입자카드번호를 받으면 이 정보에 ESC번호를 더해 출입보안서버에 보내게 된다. 즉 1바이트의 STX(Start of Text)와 8바이트의 ESC번호 7바이트의 출입자카드번호 1바이트의 BCC(Block check Character), 1바이트의 ETX(End of Text)로 구성한 데이터를 출입보안서버로 보내게 된다.

STX[1]	ESC[8]	ID Card[7]	BCC[1]	ETX[1]

그 다음 하나는 센서 데이터(GS)들이 바로 뒤를 따라 전송되게 된다. 이 GS, GC 데이터들도 1바이트의 STX, 8바이트의 ESC, 1바이트의 센서 및 제어상태, 1바이트의 BCC, 1바이트의 ETX로 구성되어있다.

STX[1]	ESC[8]	Senser & Status	BCC[1]	ETX[1]

각각의 ESC에서 데이터를 출입보안서버가 받아 출입가능여부를 파악하여 다시 ESC로 보내게 된다.

출입보안서버에서 ESC에 보내는 데이터는 1바이트의 STX, 8바이트의 ESC번호, 1바이트 GC, 1바이트의 BCC, 1바이트 ETX이다.

STX[1]	ESC[8]	GC[1]	BCC[1]	ETX[1]

여기서 BCC는 보통 사용 하는 방식인 비트검사방식인 BCC=STX xor ESC xor GC이다.

즉 STX부터 BCC전까지의 데이터를 XOR한 값을 BCC와 비교하면 된다.

AIBS시스템에 폴링(POLLING)방식을 사용하는 것은 폴링 중에 각각의 ESC에서 응답이 없을 때는 ESC와의 연결 상태가 좋지 않음을 즉시 알 수 있어 제어용에 많이 사

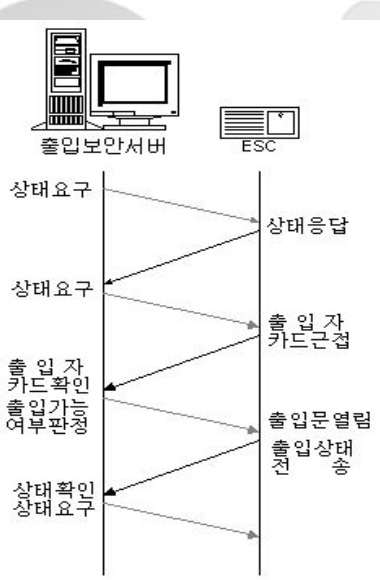


그림 2. AIBS 동작 설명

용하는 방식이다. (그림 2)는 AIBS의 동작을 간단하게 설명하고 있다.

III. 지역그룹준위 알고리즘 (AGLA : Area Group Level Algorithm)

출입문의 수가 많을수록 출입지역의 ESC개수가 많아지며 이 개수가 많아지면 출입자에 대한 지역을 효과적으로 관리하기는 매우 어려워진다. AIBS에 사용되던 출입보안서버는 (그림 2)과 같이 출입문에 대한 정보가 출입보안서버에 출입문 데이터를 보내므로 각각의 출입문 정보를 알 수 있게 되어있다.

각각의 ESC는 설치위치를 나타내고 있으며, 0에서 9까지의 숫자는 출입보안 준위를 표시하게 된다. (그림 3)에서 보면 0일 때는 그룹준위를 정하지 않은 것으로, 출입제한을 두지 않는 준위를 나타내며, 1의 그룹준위는 2보다 높으며, 9의 그룹준위가 가장 낮은 준위를 나타낸다. 출입자의 준위를 정해서 아래 그룹준위에 맞추어 입력한다. 왼쪽과 위쪽에 쓰여 진 숫자는 ESC번호를 표시하고 있으며, ESC번호가 01이면 그룹준위는 1이 되며, 57이면 그룹준위는 0이 된다. 그룹준위가 3인 출입자가 출입 가능한 ESC(출입문번호)는 15,16,25,26이 되며, 그룹준위가 4인 출입자가 출입 가능한 ESC는 54,55,64,65가 되며, 그룹준위가 5인 출입자가 출입이 가능한 ESC는 37,38이 된다.

	ESC 하위 번호
ESC 상위 번호	그 룹 준 위 기 록 X : 사용안함

	0	1	2	3	4	5	6	7	8	9
0	1	1	0	0	0	0	0	0	0	0
1	1	1	0	0	0	3	3	0	0	0
2	0	0	0	0	0	3	3	0	0	0
3	0	0	2	2	0	0	0	5	5	0
4	0	0	2	2	0	0	0	0	0	0
5	0	0	0	0	4	4	0	0	0	0
6	0	0	0	0	4	4	0	0	0	0
7	0	0	0	0	0	0	0	6	6	0
8	0	7	7	0	0	0	0	0	0	0
9	0	0	0	0	8	8	0	0	9	9

그림 3. AGLA 그룹 준위표

(그림 3)의 그룹준위표를 기초로하여 그림 3-2의 규격에 맞추어 예시표(Look up table)를 작성한다. 제일 앞쪽은 그룹준위를 기입하고, 다음은 ESC의 개수, 그 다음은 ESC 번호 열을 기입한다. 그룹준위는 0부터 9 까지이므로 그룹준위만큼의 개수가 만들어지게 된다. 그룹 준위가 1인 경우에 해당되는 ESC번호는 00, 01, 10, 11이 되며, 그룹준위 4에 해당하는 ESC 번호는 54, 55, 64, 65이 된다. 제일 앞쪽은 그룹준위를 기입하고, 다음은 ESC의 개수, 그 다음은 ESC번호 열을 기입한다.

그룹 준위	ESC 길이	ESC 번호
그룹 준위	ESC 길이	ESC 번호
-	-	-

그림 4. 예시표 구조

그룹준위는 0부터 9까지이므로 그룹준위만큼의 개수가 만들어지게 된다. 그룹준위가 1인 경우에 해당되는 ESC 번호는 00, 01,10, 11이 되며, 그룹준위 4에 해당 하는 ESC 번호는 54, 55, 64, 65 이 된다. 이런 방법으로 예시 표를 만들면 (그림 3-3)과 같다.

출입 카드(ID-Card)	그룹 준위
0001234	5
0001235	6
0001236	7
0001237	8
0001238	5
———	

그림 3-3. 출입카드 그룹준위 예시표

출입자카드(ID-Card)에 따른 그룹준위를 정해서 기록해 두고 (그림 3-3) 출입카드를 ESC에 근접 시키면,

그룹준위	길이	ESC번호
0	XX	그룹준위 1부터 9가 아닌 ESC번호
1	4	00 01 10 11
2	4	32 33 42 43
3	4	15 16 25 26
4	4	54 55 64 65
5	2	37 38
6	2	77 78
7	2	81 82
8	2	94 95
9	2	98 99

그림 3-4. 완성된 예시표

ESC번호와 출입카드번호가 출입보안서버 에 나타나게 된다. 이 출입카드번호에 해당되는 그룹준위를 찾아서 (그림 3-4)와 비교한다. 예를 들면 출입용 카드 번호가 0001235이면, (그림 3-3)에 의해 그룹준위는 6이 된다.

이 그룹준위를 (그림 3-4)의 예시표에서 비교하면, 출입 가능 한 ESC번호는 77, 78가 된다. 이런 방식으로 출입문인 ESC에 그룹준위를 만들어 넣은 후 이를 비교하는 방법으로 그룹을 정하면 간편하게 출입에 대한 보안을 구현할 수 있게 된다.[1]

Ⅳ. 구역식별알고리즘

본 논문에서 제시하는 서로 다른 ESC에서 동시에 출입자가 발생하였을 때 네트워크의 폭주로 인해 출입 가능 여부를 판정하여 출입문을 여는데 까지 다소 시간이 걸린다. 또는 그 이상 시간지연이 생겨 거의 네트워크 상태가 마비에 가까울 정도로 폭주가 일어나는 경우도 종종 발생한다.[9]

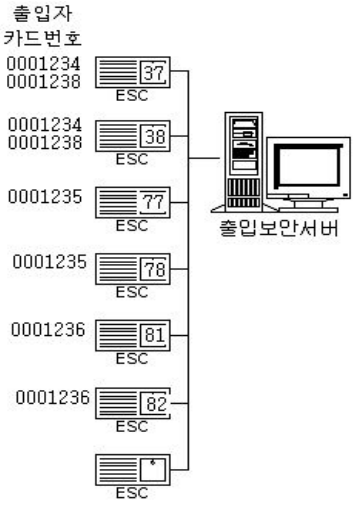
이를 방지하기 위해 ESC내에 간단한 데이터베이스를 두어 출입보안서버에 접근하지 않고 ESC자체에서 출입 가 능 여부를 판정하도록 설계하고 있다. 출입가능 여부를 판정하기 위해서는 위에서 설명한 AGLA를 이용한 예시 표와 출입카드 그룹준위를 가지고 있어야 한다. 위의 데이터를 모두 가지고 있기는 ESC가 너무 커지게 되어 IZA에 의해 아주 작은 데이터만 가지고 모든 제어를 판정하게 된다.

IZA는 출입카드그룹준위와 예시표를 비교하여 각각의 ESC에 출입 가능 한 출입자카드번호만 보관하게 된다.

(그림 4-1)를 보면 각각의 ESC에 출입자카드번호가 기록 되어 있다. 이 데이터는 출입보안시스템에서 각각의 ESC에 필요한 출입자 카드만 선택하여 전송하여 ESC의 DB에 보관해 놓게 된다.

보관된 데이터는 출입자카드를 ESC에 근접 시켰을 때 ESC에 저장된 출입자카드번호와 근접되어 읽혀진 출입 자 카드번호를 비교하여 출입문 을 개폐한다.

ESC의 번호가 37인 경우 구역식별알고리즘 IZA를 만드는 방법은 (그림 3-4)에서 ESC번호를 검색 해 보면 그룹준위 5가 된다. 그룹준위가 5에 해당되는 출입자 카드 번호는 0001234와 0001238이 해당되며(그림 3-3), 이 출입자 카드 번호를 ESC 37의 데이터 베이스에 저장해 놓으면 된다. ESC 38인 경우에도 그룹준위가 5이므로 출입자 카드번호가 0001234와 0001238이 저장되게 된다.



.그림 4-1 IZA에 의해 ESC에 등록된 카드번호

ESC 번호가 81일 경우 그룹준위가 7에 해당되며 해당되는 출입자 카드번호는 0001236이 된다. 이런 방법으로 출입자에 대한 정보를 각각의 ESC에 전송하는 방법을 구역식별알고리즘이라 한다. 완성된 IZA는 (그림 4-1)에 보였다.

Ⅴ. 실험 및 고찰

ESC에는 출입카드 리더기와 출입문제어기, 출입문 센서가 부착되어 있고, 출입보안서버는 IBM-PC 호환 기종에 윈도우2000를 사용하였다. ESC의 메인보드는 모토로라 32BIT 프로세서인 MPC860을 베이스로 하여 설계 하였으며, 사용된 OS는 Linux 커널을 포팅 하였다.

MPC860 메인보드는 기본메모리에 SDRAM 64M 바이트로 설계하였으며, Flash메모리는 8M바이트를 2개 사용하 여 1개는 커널 및 부트로더(boot loader)를 올렸 고, 다른 하나는 MTD(Memory Technology Device)를 가능하게 하여 Flash메모리를 외장 하드 디스크 처럼 사용 할

수 있도록 하였다. MTD를 사용함으로써 원격으로 제어 용 프로그램을 자유롭게 바꿀 수 있게 되었다. 데몬(Daemon)은 FTP 서버 데몬 과 Tenet 데몬 을 올 렸 으며, 이 또한 원격으로 ESC를 직접관리하기 위함이 다. ESC는 건물 내에 어느 곳 이든 출입문이 있는 곳 이면 출입문 1개당 ESC 1개가 꼭 부착되어 있으므로 실험자가 각각의 ESC로 이동하여 프로그램을 바꾸기 위해 ROM을 교체하지 않고 출입보안서버에서 원격으로 각각의 ESC의 프로그램을 바꿀 수 있도록 하였다. 50개 의 ESC와 출입자카드 100장, 출입자 30명이며, 출입 보안서버의 데이터베이스에 등록된 출입자명단은 10만 명으로 정하였으며, 그 중에 100명의 출입자를 검색하도 록 하였다. 출입자 명단을 10만 명으로 정한 것은 DB의 검색 시간 을 지연 시켜 보기 위해 DB양을 늘린 것이다. 10만 명 의 출입자명단을 IZA에 의해 각각의 ESC에 FTP와 telnet를 통해 전송하였고, 100명의 출입자 카드 정보는 각각 ESC에 포함되도록 하여 출입문의 개폐가 이루어지도록 하였다. 그리고 등록되지 않은 출입자카드 20명분과 등록된 100명분의 카드를 썩어 무작위로 30명에게 각각 4 장씩 나누어 주었다. 4장씩 가진 출입자 30명은 각각 ESC에 위치하게 하고 신호에 따라 가지고 있던 카드를 동시에 ESC내의 카드 리더기에 근접시키도록 지시하였다.

기존의 보안서버의 DB에서 출입자 정보를 찾는 방식에 비해 IZA 방식 높은 인식 속도를 보였다.

30명이 동시에 ESC에 카드를 근접 했을 때 기존방식은 30명중 가장 늦게 출입문을 개폐해준 시간은 0.8초 지연되어 출입문이 개폐되었으며 IZA방식은 적용한 시스템은 0.1초 내에서 출입문이 개폐되었다.

또한 기존 시스템에서는 보안서버의 성능에 많은 영향을 받고 있으나 IZA방식의 시스템에서는 성능에 큰 영 향을 주지 않았다.

Ⅵ. 결론

본 연구에서는 출입통제시스템에 연결된 ESC 단말기들의 과다한 데이터양에 따른 네트워크 정보 폭주를 막기 위해 논문에서 제안한 IZA를 확인하는데 있다.

30명의 출입자가 무작위 카드를 4장씩 보유하게 하여 신호 에 따라 ESC에 카드를 접근하도록 하여 실험한 결 과 IZA를 사용하지 않은 빌딩 출입 보안 시스템은 출입 문을 개폐하는데 약 10초가 걸린 반면 IZA를 이용한 출 입보안 서버는 출입문을 개폐하는데 걸리는 시간은 약 0.5초 내로 계폐가 이루어 졌다.

10만명의 출입자명단을 출입보안서버가 가지고 있어 IZA를 사용하지 않은 시스템은 이 모든 데이터를 검색하 는 시간과 동시다발적인 출입자 카드정보로 인해 출입 보안 서버가 정보폭주로 다운되는 현상도 일어났으나, IZA를 이용한 시스템은 정보 폭주자체를 해결하였으므로 시스템 정지 현상은 일어나지 않았다.

IZA에 의해 재구성된 출입자카드번호는 각각의 ESC가 보관하고 있어 네트워크를 통해 결과 정보만 출입 보안 서보로 보내고 있어 정보폭주가 일어나지 않았음을 확 인 하였다. 그리고 네트워크가 단선, 단락 되더라도 출 입자의 출입을 방해 하는 일은 절대 일어나지 않았음을 확인하였다.

본 연구를 위해 임베디드 리눅스 보드를 직적 제작 개발하게 되었으며, 리눅스 커널도 수정 추가하였고 디바이스 드라이버를 포함한 맞춤 형 OS를 빌딩 출입 보안시스템에 적용하는 계기가 되었다.

앞으로 IZA 및 AGLA를 발전시켜 더욱 안정된 빌딩 출입 보안 시스템에 쉽게 적용 되도록 모듈화 하는 연구를 계속 진행하여 상품화 가치를 높이는 연구가 계속 되어야 한다. 또한 산업 사회에 많이 사용되고 있는 RTOS(Real Time OS) 임베디드 시스템을 외국기술에 의존하지 않도록 국내 기술 확보에 노력하는 계기가 되었으면 한다.

참고문헌

[1] 서창옥,김계국 "지능형 빌딩시스템의 성능 개선에 관한 연구" 한국통신학회논문01-26-12T-9

[2] Kane, J.W., and Kodlick, M.R. "Access denial systems : Interaction of delay elements." SAND83 - 0362 1983 ; 7.

[3] Sena, P.A. "Security vehicle barriers." SAND84 - 2593 1985 ; 12-54

[4] Baker, D.R. "Curriculum Design." In Davies, S.J., and Minion, R.R., eds., Security Supervision : Theory and Practice of Asset Protection. Boston : Butterworth - Heinemann, 1999 ; 127-133

[5] Gerard Honey. "Electronics Access Control"

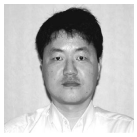
[6] Fischer,R.J., and Green, G.Introduction to security, 6th ed. Boston : Butterworth - Heinemann, 1998 ; 84 - 92

[7] Hertig, C.A. "Considering Contract Security." in Davies, S.J., and Minion, R.R., eds., Security Supervision: Theory, and Practice of Asset Protection. Boston : Butterworth-Heinemann, 1999; 227-229

[8] International Telecommunications Union(ITU). Recommendation X.200, 2000, Available at: http://www.itu.int/publications/telecom.htm

[9] Mackworth, N.H. "Researches on the measurement of human performance." In Sinaiko, H.W., ed., Selected Papers on Human Factors in the Design and Use of Control System. New York: Dover, 1961; 174-331

저 자 소 개



서 창 옥

1990년 서울산업대학교 전자공학과 공학사

1993년 건국대학교 산업대학원 전자공학과 공학석사

2001년 건국대학교 일반대학원 전자공학과 박사학위수료

~ 2003년 (주)가드텍 연구소 수석연구원

2003년~현재 메이슨 대표이사

김 계 국

원광대학교 전자공학과 졸업

숭실대학교 대학원 전자공학과 졸업 (석사)

건국대학교 대학원 전자공학과 졸업 (박사)

원광대학교 전자공학과 강사

건국대학교 전자공학과 강사

한국컴퓨터정보학회 홍보이사

한국정보기술학회 이사

문예지 시마을 신인상으로 시인등단

현재 국립 원주대학 전자통신과 교수