TETRA 시스템을 위한 안전한 소그룹과 그룹통신 서비스

이 수 연* · 정 진 욱**

요 약

무선통신 시스템의 표준으로 되어있는 TETRA(Trans-European Trunked RAdio) 시스템의 그룹 서비스와 소그룹 서비스의 안전한 통신을 위한 모델을 제안한다. 먼저, TETRA 시스템의 통신 서비스를 위해 인가된 구성원만이 데이터를 수신할 수 있어야하므로 안전한 브로드캐스팅 기술이 필요하다. 따라서, 본 논문에서 제안한 모델을 적용하면 소그룹 내부적으로 안전한 TETRA 통신 서비스를 위해 소그룹 키를 공유하고 그룹 내에서 이루어지는 TETRA 그룹통신 서비스를 위해 인가된 모든 구성원들이 안전하게 그룹 키를 공유하게 된다. 또한, TETRA 시스템의 통신서비스에서 그룹통신을 행함과 동시에 소그룹통신이 가능하게 된다.

Secure Subgroup and Group Communication Service for TETRA System

Su-Youn Lee* · Jin-Wook Chung**

ABSTRACT

This paper proposed a model supporting secure mechanism both group communication service and subgroup communication service of TETRA system that the standard developed by the technical committee Radio Equipment and Systems(RES) of the European Telecommunications Standards Institute(ETSI) provides a pure digital information technology for the transmission of speech and data. In each scheme, members in a subgroup maintains its subgroup key, which is not distributed, but computed by each member in the subgroup only with his own secret information and public values and secure subgroup members in a same subgroup can communication securely each other by using their subgroup key. Also, all members in group can share securely a group key. In communication services of TETRA system, this model supports mechanism for both group and subgroup communication are simultaneously needed.

* 천안외국어대학 컴퓨터정보과
** 성균관대학교 전기전자 및 컴퓨터공학과

1. 서 론

최근 택시회사, 군·경찰, 차량위치 추적 등에서 사용되는 무선통신 서비스인 주파수공용통신(Trunked Radio System)이 기존 아날로그방식에서 디지털방식으로 통신환경이 변화하면서 디지털 TRS에 대한 연구가 활발히 진행되고 있다. 특히, 제3세대 육상무선이동통신으로 유럽에서 제공중인 디지털 TRS 서비스인 지상중계무선통신(TETRA : Trans-European Trunked RAdio)는 ETSI(유럽 전기 토신 표준 위원회)가 PMR(개인 이동 무선 통신)과 PAMR(공공 접속 이동 통신)을 위해 지원하는 세계 유일의 무선 디지털 개방 표준이다.

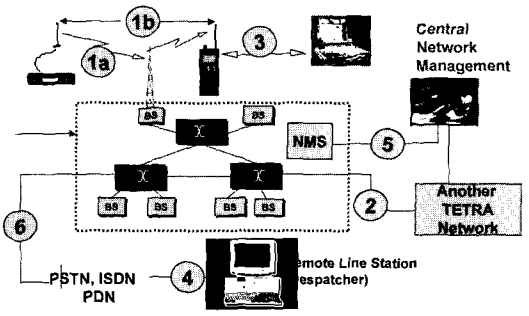
TETRA는 기본적인 음성 및 데이터의 전송 외에도 이에 부가하여 다수의 혁신적인 어플리케이션들을 지원하게 될 풍부한 기능들을 제공하는 신뢰할 수 있는 다중 매체(멀티 미디어) 이동 전송 플랫폼으로, 여기에는 GPS 인터페이스, 상태 보고(status reporting), 문자 메시지 통보, 비디오 전송, 고해상도 팩스, 전자 우편(email), 지문과 문서의 판독(scanning) 및 전송 그리고 궁극적으로는 멀티 미디어 인터넷 접속 등의 기능들을 포함하고 있다. 따라서, IP 기반의 멀티미디어 서비스를 제공하기 위한 ToIP(TETRA Over IP) 망에 대한 기술개발이 요구되고 있다.

따라서, 본 논문에서는 TETRA 시스템이 제공하는 음성과 데이터 서비스를 위해 소그룹 중심의 서비스와 그룹 중심의 서비스 구현을 위한 안전한 그룹통신 서비스 기법을 제안한다.

본 논문의 구성은 2장에서 TETRA 시스템의 서비스 구현시 필요한 안전한 통신 요구사항을 살펴보고, 3장에서는 안전한 그룹 통신을 위한 모델을 제시하여 TETRA 시스템에서 안전한 그룹 통신의 적용 예를 보여준다. 마지막으로 결론을 제시한다.

2. TETRA 시스템의 서비스 구현

지상중계무선통신(TETRA) 시스템은 기존의 주파수공용통신(TRS)에서 제공하는 서비스를 모두 제공한다.



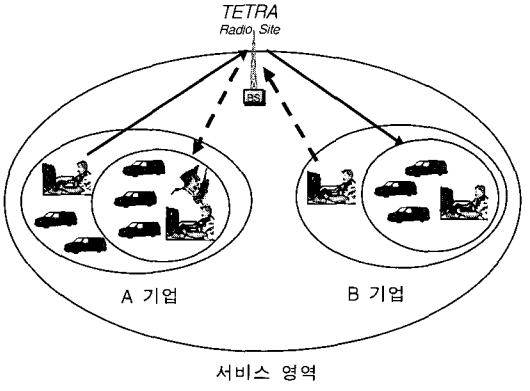
(그림 1) TETRA 시스템 구성도

(그림 1)에서와 같이 TETRA 시스템은 기존의 음성 서비스뿐만이 아니라 데이터 서비스까지도 포함하므로 PSTN, PDN, ISDN 망과도 연동이 가능하다.

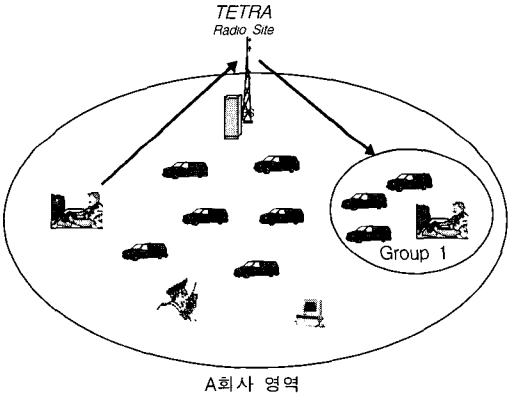
TETRA의 통신 서비스 형태로는 서로 다른 가입자기업과의 그룹으로 통신을 하는 그룹통신 서비스 형태와 동일 가입자기업에서 발신자와 수신자 그룹이 통신을 하는 소그룹통신 서비스 형태가 있다. (그림 2)와 (그림 3)은 그룹통신서비스와 소그룹통신 서비스를 나타낸다.

예를 들면, 소그룹을 형성하고 있는 기업은 기업 내부적으로 소그룹통신이 가능해야하며, 필요한 경우에는 그룹에 가입하여 그룹 키를 공유하므로 기업과 기업들간에 그룹통신이 가능해야한다. 이에 중요한 사항은 기업은 그룹통신을 행함과 동시에 기업 내부적으로 소그룹통신이 가능해야한다는 것이다. 즉, 소그룹 키와 그룹 키의 안전한 관리가 필요하다.

이와 같은 TETRA 시스템을 고려한 환경을 만족하기 위해서 구성원들은 소그룹을 이루고 이러한 소그룹들로 그룹을 형성하고 있다.



(그림 2) 그룹통신 서비스 형태



(그림 3) 소그룹통신 서비스 형태

먼저 소그룹 키 공유를 위해 각 소그룹의 구성원들은 사전 인증과정을 이용하여 소그룹 키를 안전하게 계산하게 되고, 그룹관리자와 구성원간에 그룹 키 공유는 각 소그룹내 구성원들이 공유하고 있는 소그룹 키를 공개키 방식인 Diffie-Hellman 기법으로 그룹관리자와 그룹 키를 공유하게 된다.

TETRA 시스템에서 보안 위협 요소로는 다음 사항들이 고려 될 수 있다

① 불법 사용

정당한 사용자의 번호를 도용하거나, 분실 및 도난에 의한 단말기를 불법으로 사용하여 통신사업자와 합법적인 가입자에게 과금의 혼란으로 인한 막대한 피해를 주게 된다.

② 가입자 정보의 도청 및 가로채기

무선통신의 취약성 때문에 누구든지 쉽게 다른 사용자의 통화 내용을 청취할 수 있다. 비록 암호화가 되었을 경우라도, 암호 알고리즘의 안전성이 취약하거나 관련 프로토콜이 안전하지 못할 경우도 통화내용이 도청될 수 있다.

③ 추적(traceability)에 의한 프라이버시 침해

무선통신에서는 단말기 사용자에 관한 정보 및 위치 정보가 액세스 채널에서 평문 형태로 무선 구간에 전달될 수 있다. 이런 정보들은 누가 언제 통화를 했는지 그리고 단말기 사용자의 위치 정보를 이용하여 사용자의 행방을 쉽게 추적하는데 이용될 수 있다. 제 3자 외에도 네트워크내의 인증 센터나 기지국 등이 결탁하거나, 불법행위를 할 경우, 특정 단말기 사용자의 추적은 쉽게 행하여 질 수 있다.

TETRA 시스템에서 보안 위협요소에 대처하기 위한 기본적인 보안 서비스로 고려될 수 있는 사항들은 다음과 같다.

① 인 증

무선 이동 통신에서 인증이란 통화 초기에 설정된 비밀 정보를 가입자, 즉 단말기를 소지한 자가 서비스 제공자인 네트워크에 증명하여 정당한 가입자임을 밝히는 절차이다. 이는 단말기의 불법 사용을 방지하기 위한 대책으로서 이동통신 서비스 제공자인 통신 사업자에 대해서는 반드시 고려하여야 할 보안 서비스이다. 모든 공중 통신망에서는 사용에 따른 과금이 가입자에게 징수되어야 하지만, 제공된 통화나 서비스에 대한 과금이 제대로 수행되지 않게 되거나, 다른 사람에게 과금이 되도록 하는 불법 행위들이 일어날 수 있다. 이러한 위조나 불법 사용에 대한 보호 대책을 위해 단말기 사용자의 신분 확

인이 반드시 이루어져야 한다. 이러한 인증 작업은 인증 프로토콜에 의해서 이루어 질 수 있다.

② 암 호

이동 통신은 무선 구간을 통한 이동 통신의 특성 때문에 불법 도청이 가장 용이하여 안전성 측면에서 가장 취약하다. 즉 누구든지 통화중의 내용을 쉽게 그리고 발각되지 않고 도청할 수 있다. 이러한 관점에서 무선 구간의 통화 내용은 반드시 암호화되어 보내져야 한다. 단말기 사용자의 음성 정보 및 신호 정보는 도청 및 가로채기에 대한 대책으로써 암호화가 이루어져야 한다. 이런 암호화는 암호화에 사용될 키(세션 키)가 선행되어 공유되어야 하며, 반드시 인증 절차가 완료된 후에 수행되어져야 한다.

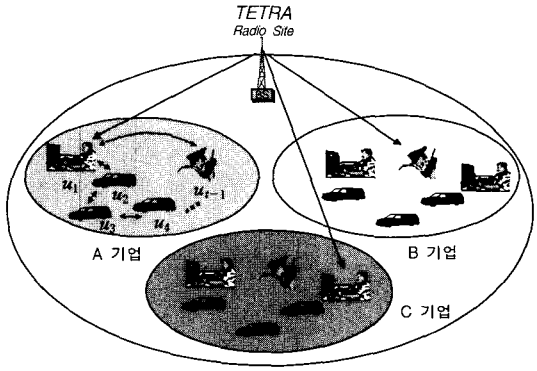
③ 추적 불가능성

추적 불가능성은 단말기 사용자의 프라이버시를 제공해 주는 기능이다. 송수신자의 위치 정보나 통화당사자에 대한 정보가 제 3자에게 노출되어 추적되는 것을 방지하기 위해서는 공개 키 암호를 사용하면 쉽게 해결할 수 있다. 그러나 공개 키 암호방식은 단말기에게 많은 계산적인 연산을 요구한다.

따라서, 이러한 보안 서비스 중 그룹 통신을 위해 소그룹 키와 그룹 키를 안전하게 공유하기 위한 분배 방식을 제안하여 TETRA 시스템에 적용하였다.

3. 안전한 TETRA 통신 모델

기존의 분배된 소그룹 관리 방식에서는 구성원이 소그룹 관리자를 전적으로 신뢰해야하는 문제점을 가지고 있다. 따라서, 본 논문에서는 이러한 문제를 해결하고자 모든 구성원들은 소그룹 키를 스스로 계산하여 그룹통신과 소그룹 통신을 동시에 수행한다.



(그림 4) 그룹 구성 및 구성원의 배열

본 논문에서 기술하는데 필요한 초기구성 및 표기 정의 <표 1>에 관해 설명한다.

≪초기구성≫

① p : 1024비트 소수.

② q : 160비트 $p-1$ 의 소인수

③ g : 위수 g는 Z_p^*의 원소이다

④ 생성자 g에 대한 법 지수연산(modular exponentiation)시에 모듈러 p상에서 생각한다.

⑤ h 를 일방향해쉬함수로 가정하고,

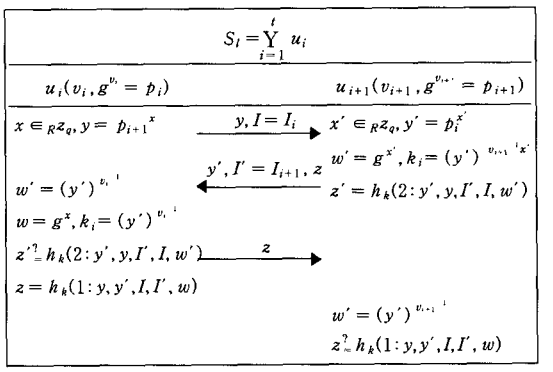
h : $\{0,1\}^* \rightarrow \{0,1\}^q$ 을 만족한다.

〈표 1〉 표기 정의

표 기	의 미
u	그룹통신을 구성하고 있는 구성원
k_i	키 동의 과정에 의한 사전 공유키
w_i	사전키를 일방향 함수의 입력값으로 계산되어진 공개정보
K_i	각 소그룹마다 구성원간에 공유되어진 소그룹키
g^{XK_i}	각 구성원과의 그룹관리자가 계산과정에 의해 얻어진 공유키 (단, : X 그룹관리자의 비밀키로 정한다.)
t	소그룹의 구성원 수

3.1 소그룹 서비스를 위한 소그룹 키 공유

3.1.1 사전인증 및 사전 공유키 공유과정



(그림 5) 구성원 u_i, u_{i+1}의 키 동의 과정

구성원 u_i, u_{i+1}은 키 동의(key agreement)과정으로 인증과 사전 공유키를 형성하고 있는데, (그림 5) 과정을 살펴보면, 먼저 구성원 u_i는 비밀키(v_i)로 공개키(p_i)를 생성하여 공개하고 구성원 u_{i+1}도 비밀키(v_{i+1})로 공개키(p_{i+1})를 생성하여 공개한다. 각 구성원들은 상대방의 공개키를 이용하여 y, y'를 계산하게 되는데, 이는 공유하고자 하는 사전 공유키($k_i = \alpha^{xx'}$)를 계산하는데 사용된다. 마지막 단계에서는 사전 공유키를 이용한 일방향 함수 값을 각 상대방에게 보내 줌으로써, 사전 공유키에 대한 확인작업(confirmation)을 수행할 수 있게되고, 이렇게 구성원들은 안전하게 사전 공유키를 공유할 수 있을 뿐만 아니라 서로 신뢰관계를 형성하게 된다.[5]

3.1.2 소그룹 키 공유과정

각 구성원들은 두 개의 사전 공유키 k_i, k_{i-1}로 공개정보 w_i를 계산하게 되는데, 이 공개정보를 이용하여 구성원들은 소그룹 키를 계산하게 된다[6].

① 구성원 u_{i-1}, u_i는 키 동의 과정으로 사전 공유키를 생성한다.

② 구성원 u_i는 사전 공유키를 이용하여 공개정보 $w_i = h(k_i) - h(k_{i-1})$를 계산한다.

- $h(k_i)$: 사전 공유키를 입력 값으로 n번의 일방향 함수를 적용한다.

③ u_i는 공개정보를 이용하여 소그룹 키 K를 다음과 같이 계산한다.

- u_i는 k_{i-1}, k_i를 가지고 있고 소그룹 키 K는 다음과 같이 구성되어있다.

$$K = h(k_i) + h(k_{t-1}) + \cdots + h(k_1)$$
$$(\text{단}, 1 \le l \le n\ )$$

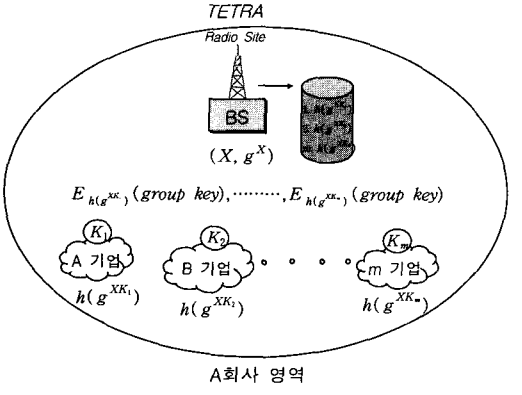
- u_i는 $h(k_{i-1})$, $h(k_i)$값을 알고 있으므로 u_{i+1}의 공개정보 $w_{i+1} = h(k_i) - h(k_{i+1})$에서 u_i는 $h(k_{i+1})$를 계산할 수 있다.
- u_i는 $h(k_{i-1})$, $h(k_i)$값을 알고 있으므로 u_{i-1}의 공개정보 $w_{i-1} = h(k_{i-2}) - h(k_{i-1})$에서 u_i는 $h(k_{i-2})$를 계산할 수 있다.
- 이와 같은 방법을 귀납적으로 적용하여 인가된 소그룹 구성원들은 K를 구할 수 있다.

3.2 그룹 서비스를 위한 그룹 키 공유

본 절에서는 그룹통신을 하기 위해 필요한 구성원과 그룹관리자간에 그룹 키를 안전하게 공유할 수 있는 방식을 제안한다.

3.2.1 공유 키 공유과정

공유키를 계산하게 되는데 인가된 구성원은 소그룹 키(K_i)를 소유하고있고 그룹관리자와 구성원간의 공유 키 공유를 위해 그룹관리자의 비밀 값과 소그룹 키를 공개키 방식인 Diffie-Hellman 방식으로 공유키를 공유하게 된다. 공유키 계산과정을 살펴보면 다음과 같다(그림 6).



(그림 6) 공유 키 공유과정

각 구성원들은 자신이 소유하고 있는 소그룹 키를 생성자(g)에 지수승한 값(g^{K_i})을 공개하게 되고, 그룹관리자 또한 자신의 비밀키(X)를 생성자(g)에 지수승한 값(g^X)을 공개하여 이를 Diffie-Hellman 방식으로 각 구성원과 그룹관리자는 공유 키 $h(g^{K_iX})$를 공유하게 된다.

3.2.2 그룹 키 공유과정

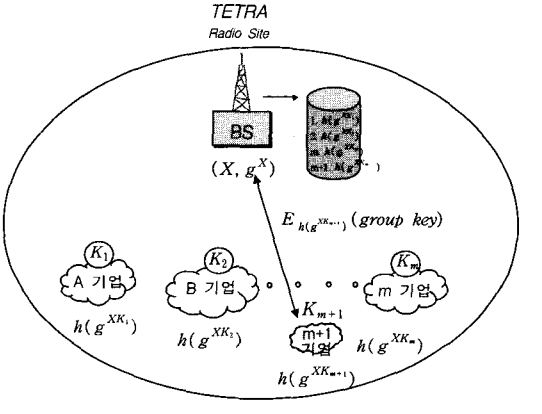
그룹관리자는 각 구성원들과 그룹 키를 공유하는 과정이다. 그룹관리자는 각 소그룹에 해당되는 공유키를 저장하고 있으므로 이를 이용하여 각 구성원들에게 그룹 키를 암호화 한 후 전송하게 된다. 소그룹 키를 소유하고 있는 구성원만이 암호문을 복호화하여 모든 구성원들은 그룹 키를 공유하게 된다.

3.3 그룹 내 서비스 영역 추가 및 철회

3.3.1 그룹 내 서비스 영역 추가

소그룹이 특정한 그룹 서비스를 원하는 경우, 소그룹은 그룹에 가입하여 안전한 그룹 통신 서비스 및 소그룹통신 서비스를 수행할 수 있어야 한다. 즉 추가된 서비스 영역에 있는 구성원들은 추가되기 이전의 전송된 데이터를 수신할 수 없어야하므로 이러한 암호학적 보안을 만족하기 위해 그룹 내에서 사용되어졌던 그룹 키를 갱신해야만 한다.

소그룹 내에 있는 각 구성원들은 사전에 계산된 소그룹 키를 이용하여 그룹관리자와 공개키 방식인 Diffie-Hellman 방식으로 공유키를 공유하게 된다. 이 때, 그룹관리자는 갱신된 그룹 키를 가입한 소그룹의 공유키로 암호화하여 전송하고, 나머지 소그룹은 기존의 그룹 키를 입력으로 일방향 함수 값을 계산하여 갱신된 그룹 키를 얻게 된다.



(그림 7) 그룹 내 서비스영역 추가

3.3.2 그룹내 서비스 영역 철회

그룹 통신 서비스 영역에서 특정 서비스 영역을 철회하는 경우, 즉 특정 소그룹 영역은 그룹영역에서 탈퇴하게 되고 서비스 영역에서 철회된 영역에서는 더 이상 암호화된 데이터를 복호화 할 수 없어야한다. 따라서 그룹에서는 기존 그룹 키를 갱신해야만 한다(그림 6).

이때 키 갱신과정에 참여하는 그룹관리자는 모든 소그룹 영역의 구성원들과 공유키를 저장하고 있다. 따라서 그룹관리자는 철회된 소그룹 영역의 공유키를 제외한 나머지 구성원의 각각의 공유키로 갱신된 그룹 키를 암호화하여 전송하게 된다.

4. 결 론

본 논문은 TETRA 시스템에서 안전한 그룹 통신을 위해 소그룹 키와 그룹 키의 안전한 관리를 위한 모델과 수시로 변경되는 그룹환경에 유연하게 대처할 수 있는 기법을 제안하였다. 즉, 구성원 스스로 소그룹 키를 계산하게 되므로 신뢰기관에 독립적으로 그룹 통신 및 소그룹 통신을 운영 할 수 있다. 따라서, 제안한 방식으로 제 3세대 육상무선이동통신으로 유럽에서 제공중인 디지털 TRS 서비스인 지상중계무선통신(TETRA : Trans-European Trunked RAdio)의 그룹통신 및 소그룹 통신이 안전하게 이루어지므로 보다 다양한 서비스를 제공할 수 있다.

참 고 문 헌

[1] 조태남, 이상호 "(2,4)-트리를 이용한 그룹키 관리", 정보보호학회지논문지, 제4호, 2001. 08.

[2] Chung Kei Wong, Mohamed G. Gouda, Simon S. Lam, "Secure Group Communications Using Key Graphs", Proceedings of the {ACM} {SIGCOMM} '98 conference on Applications, technologies, architectures, and protocols for computer communication.

[3] S. Setia, S. Koussih, S. Jajodia, E. Harder, "Kronos : A Scalable Group Re-Keying Approach for Secure Multicast", In 2000 IEEE Symposium on Security and Privacy.

[4] A. Perrig, D. Song, J. D. Tygar, "ELK, a New Protocol for Efficient Large-Group Key Distribution", IEEE Symposium on Seurity and Privacy, Oakland, CA, USA, May 2001.

[5] M. Just, S. Vaudenay, "Authenticated Multi-Party Key Agreement", In Advances in Cryptology - ASIACRYPT'96, LNCS 1163, Springer-Verlag, pp.36-49, 1996.

[6] 이수미, 이동훈, "분배된 소그룹 관리 방식에서 제한된 권한을 갖는 신뢰기관", 고려대학교 대학원, 2003. 2.

[7] ETSI ETS 300 396-1 : Terrestrial Trunked Radio(TETRA) ; Technical requirements for Direct Mode Operation(DMO) ; Part1 : General Network Design.

[8] ETSI TETRA specification, ETS 300 392-1, ETS 300 392-2.

[9] "Extension of EPT Terms of Reference to Enable TETRA 'Release 2'", ETSI Board #2, Sophia Antipolis, September 2000.

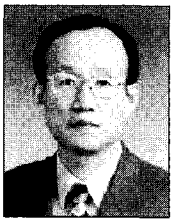
이 수 연

1990년 단국대학교 전산학과 학사

1993년 단국대학교 전산통계학과 석사

1997년 성균관대학교 전기전자 및 컴퓨터공학과 박사수료

1997년~현재 천안외국어대학 컴퓨터정보과 교수



정 진 욱

1974년 성균관대학교 전기공학과 학사

1979년 성균관대학교 대학원 전자공학과 석사

1991년 서울대학교 대학원 계산통계학과 박사

1982년~1985년 한국과학기술 연구소 실장

1981년~1982년 Racal Milgo Co. 객원연구원

1985년~현재 성균관대학교 전기전자 및 컴퓨터공학과 교수